2004-09

Prototype system for detecting and processing of IEEE 802.11G signals

Kypriotis, Georgios

Monterey California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PROTOTYPE SYSTEM FOR DETECTING AND PROCESSING OF IEEE 802.11G SIGNALS

by

Georgios Kypriotis

September 2004

Thesis Advisor:	Tri T. Ha
Second Reader:	David C. Jenn

Approved for public release, distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Prototype System for Detecting and Processing of IEEE 802.11g Wireless Signals			**5. FUNDING NUMBERS**
6. AUTHOR(S) Georgios Kypriotis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

On the modern battlefield, successful and fast communications is a critical issue. So the need for transmitting information in larger amounts through a military high-speed network increases. Thus the military is seeking viable and effective solutions that may fulfill these requirements in an operational environment.

This thesis develops a prototype system based on appropriate low-cost software and hardware solutions. This system is able to detect, analyze and process wireless 802.11g signals. The evaluation of the newly designed system proved that it is effective up to distances of about 400 m with a low packet error rate and could be a useful tool for detecting wireless 802.11g networks. After evaluating the system, it was used for capturing wireless signals so that we would determine the effective transmission range and the data throughput of an 802.11g network. We determined that such a wireless network could be used in military operations because it offers high data rates up to 200 m, while it maintains a connection of the wireless clients for distances up to 400 m. In addition, the performance data collected can be used as guidelines for estimating the expected performance in an operational situation and can provide useful information for successful planning.

14. SUBJECT TERMS Wireless Transmission Protocol, IEEE 802.11g, Wireless LAN, Data Throughput, Transmission Rate			**15. NUMBER OF PAGES** 115
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

PROTOTYPE SYSTEM FOR DETECTING AND PROCESSING OF IEEE 802.11G SIGNALS

Georgios Kypriotis
Lieutenant, Hellenic Navy
B.S., Hellenic Naval Academy, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING
AND
MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Georgios Kypriotis

Approved by: Tri T Ha
Thesis Advisor

David C. Jenn
Second Reader

John P. Powers
Chairman, Department of Electrical and Computer Engineering

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

On the modern battlefield, successful and fast communications is a critical issue. So the need for transmitting information in larger amounts through a military high-speed network increases. Thus the military is seeking viable and effective solutions that may fulfill these requirements in an operational environment.

This thesis develops a prototype system based on appropriate low-cost software and hardware solutions. This system is able to detect, analyze and process wireless 802.11g signals. The evaluation of the newly designed system proved that it is effective up to distances of about 400 m with a low packet error rate and could be a useful tool for detecting wireless 802.11g networks. After evaluating the system, it was used for capturing wireless signals so that we would determine the effective transmission range and the data throughput of an 802.11g network. We determined that such a wireless network could be used in military operations because it offers high data rates up to 200 m, while it maintains a connection of the wireless clients for distances up to 400 m. In addition, the performance data collected can be used as guidelines for estimating the expected performance in an operational situation and can provide useful information for successful planning.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I must acknowledge the constant and unconditional support I received throughout this project from my loving wife Maria without whom this work could have never been completed. Moreover, I am also grateful to my two sons, Vassilis and Ioannis-Nikolaos, for the patience they showed for my absence during my research at the Naval Postgraduate School.

I also wish to dedicate this thesis to my thoughtful and supportive parents, and especially to the memory of my father who always tried to teach me the real values of life.

I would like to express my sincere appreciation to my advisors Professor Tri Ha who provided me his guidance along the way and Professor David C. Jenn who immediately agreed to be my second advisor. I would also like to thank Nathan Beltz, the Cryptologic Research Lab Manager, for his technical assistance and for all the needed equipment for this research.

Thanks go out as well to Ron Russell for his help in editing my thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The IEEE announced the IEEE 802.11g, its latest standard, in April 2003. A major advantage is that it offers backward compatibility with the earlier IEEE 802.11b standard, and it also supports a maximum transmission rate of 54 Mbps with better granularity between the lower rates than all the other IEEE standards. Due to the high transmission rate, a wireless 802.11g military network may be a successful solution during operations in an open-area battlefield.

This thesis presents the basic characteristics of the 802.11g and the similarities to the other two IEEE standards. Based on the transmission environment and on the specifications of the wireless network we intended to built, two theoretical path loss models are briefly analyzed. We present the free-space path loss model and the two-ray path loss model. Their theoretical results were a metric for the experimental results of the path loss that are presented in the following chapters.

Firstly, we built a prototype laptop-based mobile system that is capable of detecting, analyzing and processing 802.11g wireless signals. This mainly consisted of a Dell laptop, a software network analyzer installed in the laptop, and a wireless card that would operate as the receiver. AiroPeek NX software was chosen as the protocol analyzer, based on its price and on previous efficient implementations. Next, we tested three wireless cards: the Linksys WPC54G, the Orinoco Gold 11a/b/g combo card and the D-Link DWL-650, executing extensive measurements. We tried all three security combinations offered by the IEEE, that is, using no WEP, using a 64-bit WEP and using a 128-bit WEP. The experimental environment was a flat beach area, and we maintained the LOS between the source and the receiver. The Orinoco wireless card proved to be more efficient than the other two due to its low packet error rate.

Secondly, we evaluated the performance of the newly designed system to make sure that it was effective in an open-area environment. Again, based on experimental measurements, we used the “packet sniffing” technique against three different wireless systems. Each system consisted of an access point and a wireless card. Thus, the effective

reception range of the system was about 400 m from the source. The packet error rate became significant (5%) after the distance of 200 m and its maximum value was 11.5% at the maximum distance of the 400 m. So the system proved to be an effective tool for analyzing and capturing wireless 802.11g signal outdoors and could be used during military operations.

Next, using this system we evaluated the performance of a very simple 802.11g WLAN that was formed by one AP and one wireless client. The exchange of small data (32 bytes) and of the corresponding ACK packets was measured so that we could determine the range-transmission rate profile of the 802.11g outdoors. We determined that such a WLAN offers 40 Mbps at close distances (70 m) from the AP while the transmission rate remains high with a value of 20 Mbps at 200 m from the source. The interconnection of the participating units is maintained up to 400 m but the transmission rate decreases to about 2 to 1 Mbps, as expected.

Lastly, using the analysis capability of the designed system, we computed the actual data throughput of the WLAN. This process showed that although the overhead bits of a wireless packet are indispensable, they decrease data throughput. The actual data transmission rate is almost 3.5 times less than the advertised 54 Mbps. For ranges close to the AP its value is 15 Mbps; while at 400 m it decreases to about 0.5 Mbps. Of course a data throughput of 15 Mbps is still a significantly high rate that can be used in military operations.

I. INTRODUCTION

A. PURPOSE OF WIRELESS

Over the past few decades a promising new technology has taken advantage of frequency spectrum to create a very accessible type of Local Area Network (LAN). During the last few years, Wireless Local Area Network (WLAN) technology has become a very practical and affordable networking technology. Their applications keep growing and have become very popular. Some of the most important applications of the WLANs are the following:

- Connection/Extension of the wired LANs: The wireless networks are used so that we achieve the connection of the users with the basic element (backbone) of the wired networks. In such a case we do not need to use any wires for installation, which is extremely difficult and costly during installation.
- Building Interconnection: The technology of the wireless networks can lead to building interconnections. The devices normally used to achieve this are called routers or bridges.
- Sporadic Access to a Network: It is desirable to establish wireless networks in public places, such as libraries, airports, educational institutes or offices, where many users may want to have access to the wired network of each specific corporation. Of course, in such cases, security of the data is a very important issue.
- Creation of Ad-Hoc Networks: The ad-hoc networks are decentralized peer-to-peer networks, which are usually created to meet a specific situation or need. Such networks may be used in symposiums or in classrooms, where the clients or students can exchange data and information through the temporary wireless networks, without installing any special equipment.

In comparison with the wired LANs, WLANs have the following advantages:

- Wide Mobility of the Users: This is the most obvious advantage offered by a WLAN. Of course the user has to own the proper portable device (a laptop with a wireless card adapter or a PDA).
- Easy and Quick Installation: Becoming a wireless client to a WLAN requires little effort. Moreover, creating a WLAN is not a rigorous procedure. On the contrary, LANs require installation of wires, which is not an easy procedure.
- Robustness: A wireless network can survive disasters. This means that if the wireless devices survive, people can still communicate with each other, without concern about damaged wires or damaged connections.

- Flexibility: WLANs can be extended easily, since the access medium is accessible everywhere. They can also be adjusted to various needs of their users, depending on each specific case. Also, within radio coverage, nodes can communicate without further restrictions.
- Cost: In some cases the WLAN solution is cheaper than the traditional LAN. One very characteristic example is the use of the wireless equipment for the point-to-point communication between two buildings or two corporations, compared to the cost of a private line. In addition, the long term cost of maintenance is less than a wired LAN.

Nowadays the advantages of wireless networks are being examined as to whether they could be employed for military operations, for which the mobility of the users, the security and integrity of data, and the high data transmission rates are very important issues.

At the same time, using WLANs in the military increases security risks due to the vulnerability of the WLAN physical layer to exploitation. Various studies have been published that describe several theoretical vulnerabilities in the security mechanisms provided by the 802.11 standards. Attacks based on these vulnerabilities have been implemented and are freely available on the World Wide Web.

B. SCOPE OF THESIS

The later IEEE standard 802.11g operates in the 2.4-GHz frequency band and uses Orthogonal Frequency Division Multiplexing (OFDM). It seems an increasingly attractive option as a high-speed information network for military use, providing a theoretical maximum transmission rate of 54 Mbps. The 802.11g generates excitement because it offers the greatly improved speeds of 802.11a, but it is also backwards compatible with existing 802.11b networks. In addition, the new security mechanism that is implemented in the 802.11g is a really promising feature and increases the security in a potential military wireless network.

This thesis investigated commercially available 802.11g compliant hardware and software. The research includes building a low-cost prototype system that will be helpful for military applications, either as a detection system or to process other 802.11g WLAN signals in the battlefield. Furthermore, the system is a useful tool for assessing the security vulnerability of a military WLAN network.

Another goal of this research was that the prototype system was to be capable of collecting data pertaining to the detection range and effective data rate of the 802.11g WLAN at various ranges. Finally the actual data throughput of the 802.11g was estimated.

The final product of this research was a prototype system, composed of commercially available low-cost hardware and software, which can be used to detect and to process 802.11g compliant WLAN signals. In addition, the performance data collected by the prototype system can be used as a guideline for predicting expected performance in an operational scenario and can provide valuable information for proper deployment planning.

The thesis is organized as follows. Chapter II briefly analyzes the 802.11 architecture and the basic wireless components. Then a brief description of the new IEEE 802.11g standard is presented. The two theoretical propagation models that are described are useful background information needed to understand and to compare the experimental data collected.

Chapter III explores the development of the prototype system. All the appropriate requirements for the development of the prototype system are presented. These include the selection of the hardware and the software of the system. Most importantly, the wireless card that was used as the basis of the receiver was chosen. Chapter IV evaluates the performance and the test results of the prototype system when it is used to detect and to process 802.11g WLAN signals, including range metric and error performance. Chapter V covers the test setup and measurement results of the 802.11g link performance implementing the evaluated prototype system. Finally the actual data throughput was calculated in order to compare it with the theoretical advertised values. Chapter VI presents a summary with conclusions and proposes prospective developmental work in this area.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter analyzes the basic characteristics of the IEEE standard, the basic components of a corresponding wireless network and the main wireless topological forms. Then, it briefly presents the new IEEE standard, the 802.11g and some important differences and similarities with the former IEEE standards. Finally this chapter contains the two theoretical path loss models that will be used as a metric for the experimental measurements so that we make the correct choices for the development of the prototype system, which is the main purpose of this thesis. This experimental research will be presented in the following chapters.

A. IEEE 802.11 INTRODUCTION

The IEEE started the 802.11 project in 1990 with a scope "to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area." [1] The IEEE 802.11 standard was formally announced by the IEEE in 1997. Then the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards in 1999. The goal was to develop a technology based on standards that could use various frequencies, modulation schemes, encoding forms and applications, similar to the 802.3 Ethernet standards. [1]

In 2003, the latest approved standard of IEEE was announced, the 802.11g. Nowadays WLANs based on this technology are becoming very popular. Simultaneously all wireless communication vendors are trying to develop relevant accessories.

The IEEE 802.11 standard specifies the use of both Radio Frequency (RF) spread spectrum and infrared technologies for WLAN. The RF spread spectrum technology was initially divided into two components, Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Later a more efficient modulation technique was implemented, the Orthogonal Frequency Division Multiplexing (OFDM), as shown in the Figure 1 below. [1,2]

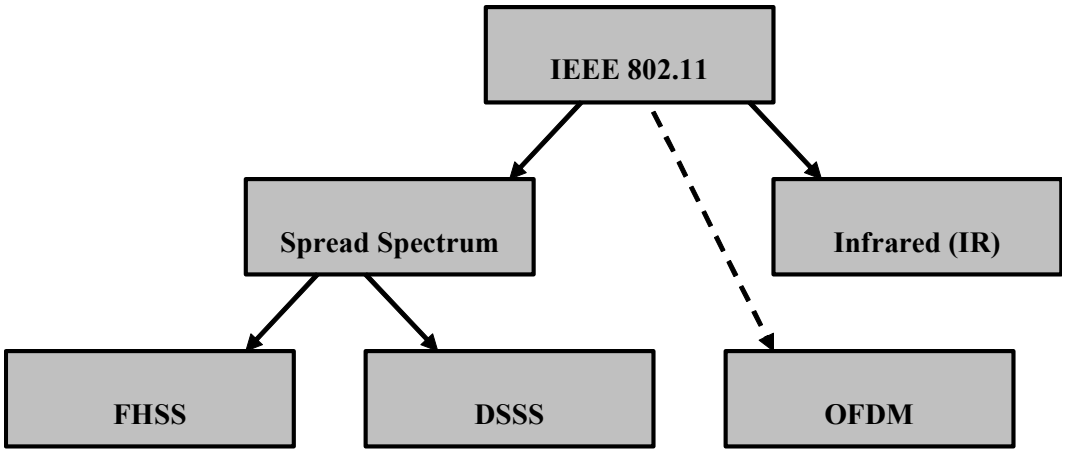

Figure 1. IEEE 802.11 WLAN Technologies (After Ref. 1.)

It is worth pointing out that although various 802.11 standards aim for data rates of up to 54 Mbps, the effective data throughput of all standards is usually less than 50% of the maximum theoretical data rates. This is due to the nature of radio transmissions using half-duplex communications and the need for overheads for coordination, error correction and other management functions. It is also worthwhile to note that advertised ranges are widely variable and can be affected, often drastically, by all types and manners of obstructions. [2,3]

B. IEEE 802.11 ARCHITECTURE

1. Layering

The 802.11 referred to the two lower layers of the Open System Interconnection (OSI). That is, it referred to the Physical Layer (PHY) and to the Medium Access Control (MAC), one of the two sub-layers of the Data Link Layer. The other Data Link sublayer, named the Logical Link Control (LLC), is the standard model IEEE 802.2. It cooperates with all the different MAC of the IEEE 802 standard, as we can see in Figure 2. [1]

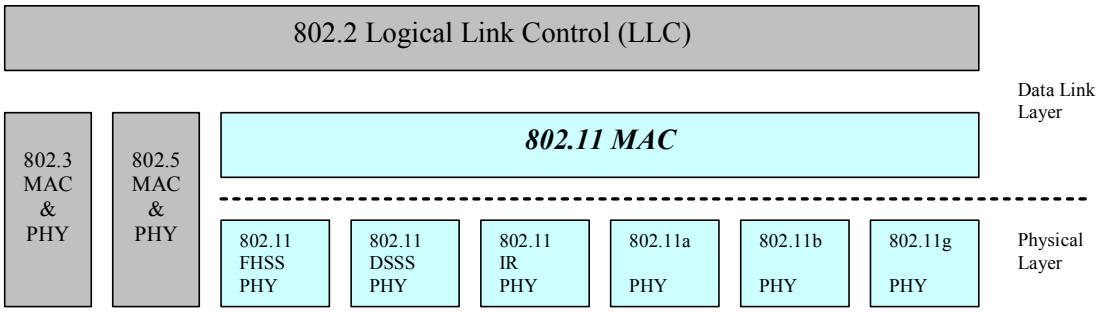

Figure 2. Layering of the Standard 802.11 (After Ref. 1.)

The whole concept, which is implemented by the standard 802.11, is that there is only one MAC. This MAC is responsible and able to support more than one Physical Layer. Each Physical layer is divided into two more sublayers, as we can see in Figure 3.[1]

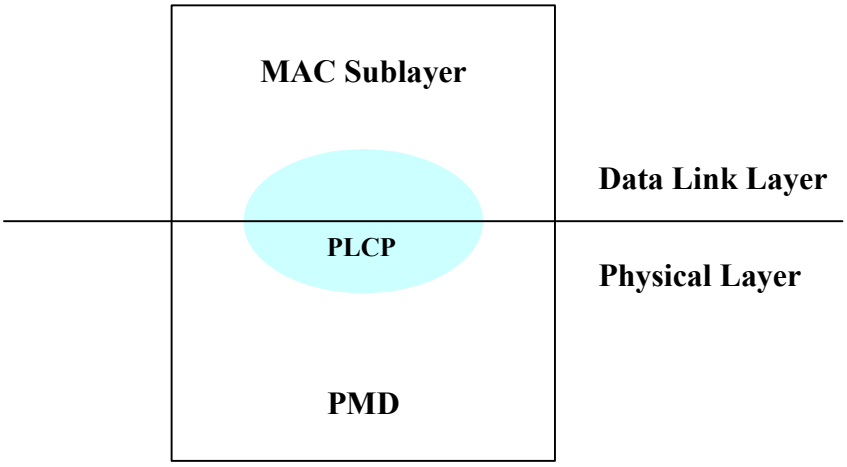

Figure 3. Physical Layer of Standard 802.11 (After Ref. 1.)

The Physical Layer Convergence Procedure (PLCP) sublayer is used for the co-operation of the various Physical Layers with the common MAC. The sublayer Physical Medium Dependent (PMD) contains all the appropriate operations needed for the transmission of the information from each specific Physical Layer. [1]

2. Basic Wireless Components

The Wireless Networks, which use the standard 802.11, consist of the following four basic units:

- Access Point (AP): An Access Point is a physical device that allows wireless users to access a wired network. Thus, APs are designed to act as the wireless equivalent of an ethernet hub or switch. They allow multiple wireless clients to connect to one central hub in Infrastructure Mode. Basically this means that from the physical connectivity point of view they act as a star network. Every wireless client talks to every other one via the AP. Finally, access points act as a central transmitter and receiver of WLAN radio signals. [1]
- Distribution System: To enable roaming between multiple access points and connections to wired network resources, the 802.11 standard specifies a distribution system, which provides wired or wireless interconnections between access points. The 802.11 standard says that the distribution system may be of any technology, such as Ethernet, token ring, or any other network type. The majority of actual installations, however, use Ethernet. [1]
- Wireless Medium: Various Physical Layers have been established, and they use either radio frequencies or infrared rays, for the transmission between the stations of the wireless network.
- Wireless Stations: The stations or wireless clients exchange the information through the wireless network. They are usually portable devices, such as laptops.

3. Service Sets

a. Basic Service Set (BSS)

The basic topological form of each 802.11 is called Basic Service Set (BSS). The limits of the BSS are established from the area of coverage, which is called Basic Service Area (BSA). A station that belongs to a specific BSS is able to communicate with any other station, which belongs to the same BSS. [1]

A BSS uses a single cell and a single Service Set Identifier (SSID), the network name. When using only one AP, the network is in infrastructure mode by default. In infrastructure mode, when one wireless client transmits packets to another wireless client, the data must go through the AP.

An example of a very simple BSS is shown in the Figure 4, where an AP is connected to the wired LAN and all the wireless stations (STA1, STA2 and STA3) communicate directly with that AP.

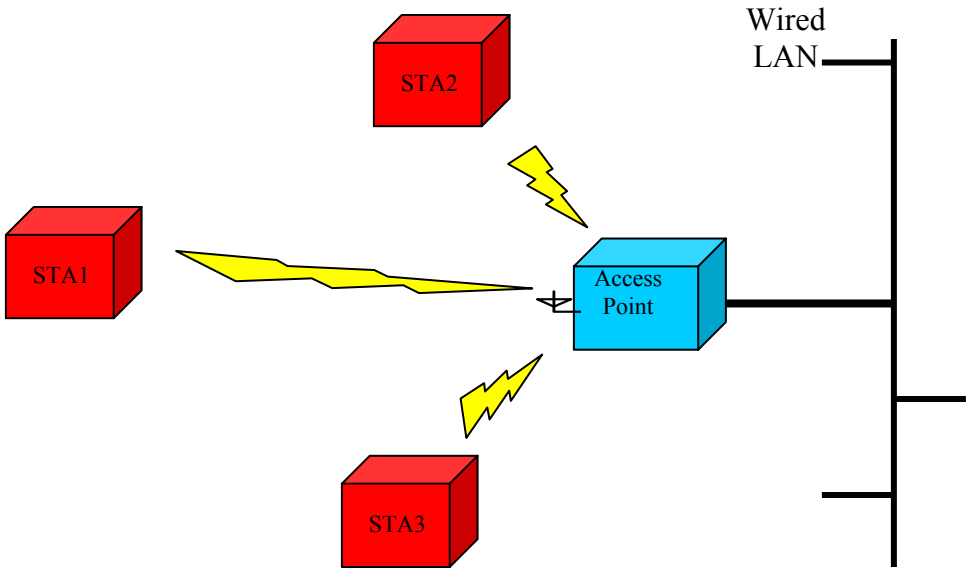

Figure 4. Topology of a BSS

b. Independent Basic Service Set (IBSS)

An IBSS is an IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless mobile stations and no access point. An IBSS has a single cell and one SSID. It is an independent network with each station communicating directly with all the other ones. Client stations connect directly to each other much like the wired peer-to-peer network. The BSS in this case is called Independent BSS (IBSS) or an ad hoc BSS or, even simpler, an ad hoc network because it can be constructed quickly, without much planning, and has no access point with which to connect. The IBSS is composed of at least of two stations, and it is usually temporary. That means it is formed for a specific purpose, without pre-planning, and then it is decomposed when the use of the LAN is not needed any more. [1]

Figure 5 shows an IBSS. There are three wireless clients (STA1, STA2 and STA3) inter-connected to each other. They are able to communicate and exchange wireless packets without the presence of any AP.

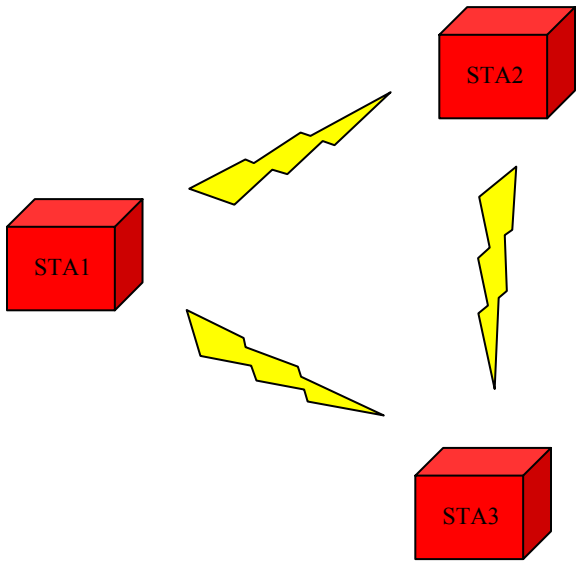

Figure 5. Topology of an IBSS

c. Extended Service Set (ESS)

In an infrastructure network, a number of BSSs can be connected to each other, forming an Extended Service Set (ESS). An ESS must have at least two access points so that it consists of at least two cells. We can accomplish this by connecting the APs of these BSSs through a wired or wireless network. In that way, we accomplish the communication between stations that belong to different BSSs but they are part of the same ESS. The ESS is finished when there is a station between the APs which operates in a higher layer, a router for example. [1]

The ESS does not have to support roaming, although roaming is allowed and sometimes required, based on the user needs. Roaming can be seamless or non-seamless depending on how the network is configured and the range of each of the access points. When the cells of the access points overlap, the users can roam from one cell to another without losing network connectivity. [1]

Figure 6 illustrates an ESS, formed by two non-overlapping BSS. Obviously, the APs of these BSSs are connected to each other and both of them are connected to the wired LAN.

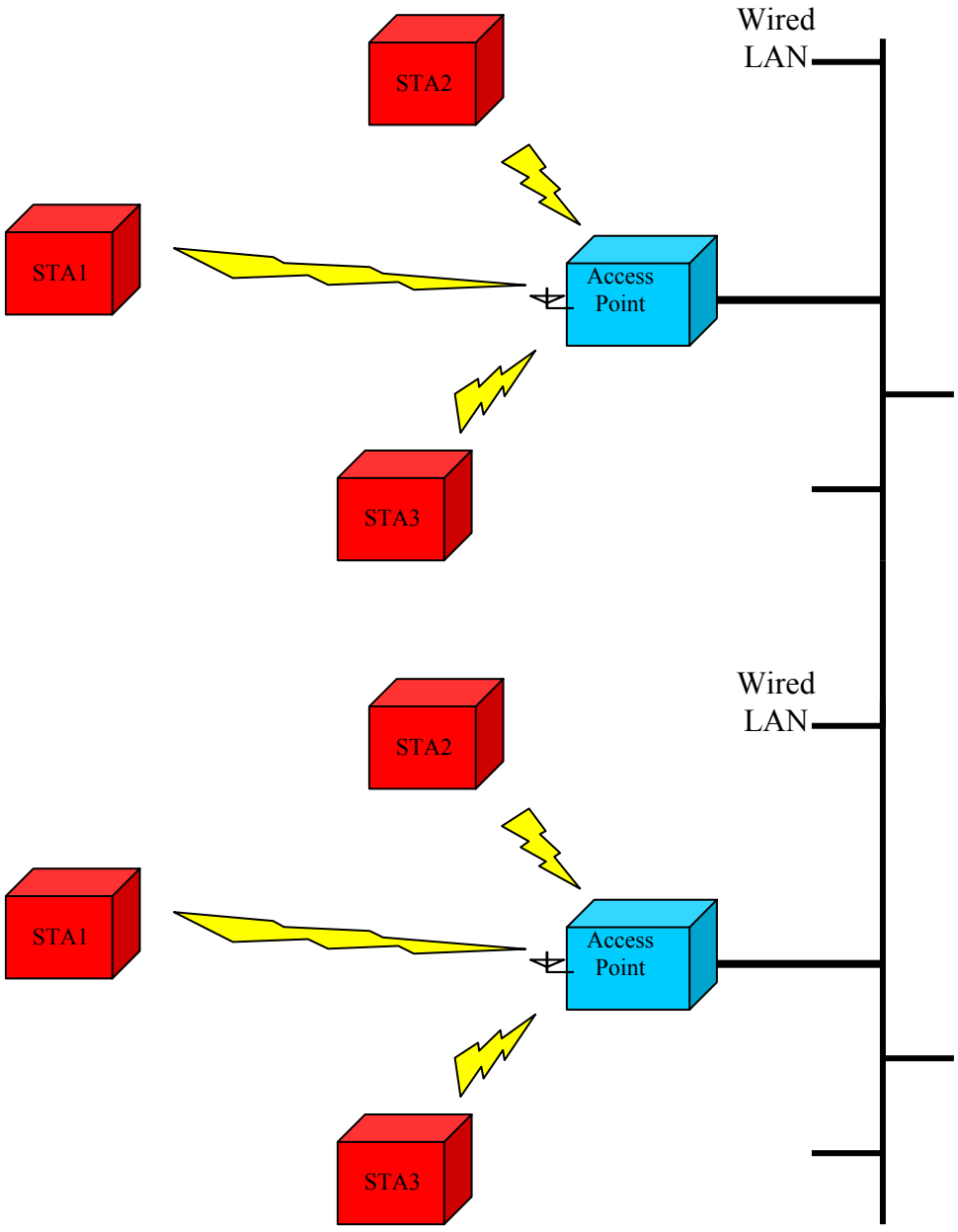

Figure 6. Extended Service Set

d. Distribution System

The Distribution System has a very significant role in the functionality of the 802.11, although its implementation is not described in the IEEE standard documenta-

tion. Only the services that have to be provided to the wireless stations are described. As we already mentioned, the distribution system is responsible for the inter-connection of the APs, that is, the connection of the BSSs and the formation of the ESSs. Thus, in that way, the exchange of the packets between the stations, which belong to different BSSs and within the same ESS, is possible. The distribution system may be wired or wireless.[1]

We can see an example of a distribution system in Figure 7.

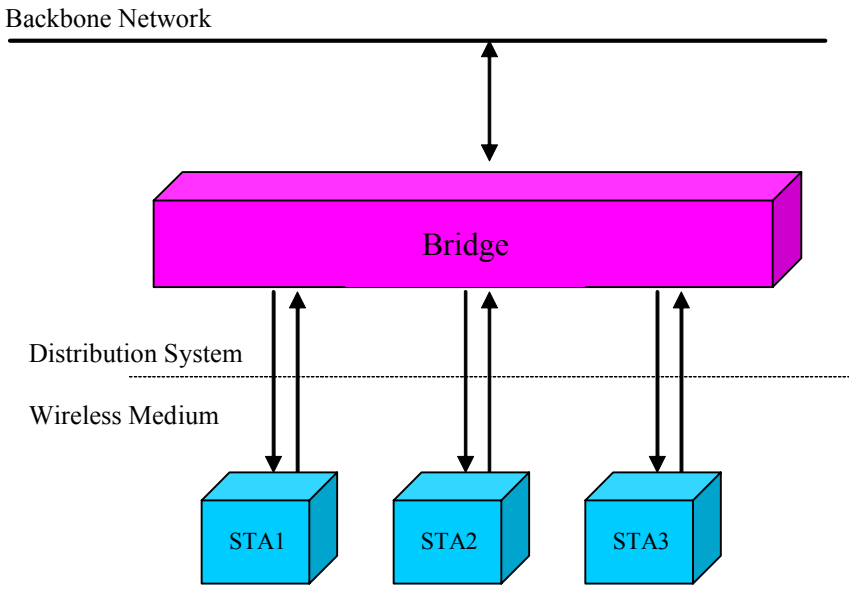

Figure 7. Distribution System

The APs operate as bridges between the distribution system and the wired network. If the station STA1 tries to transmit a packet to another station (i.e. STA2), it first must go to the corresponding AP. Then the packet is transformed into a type of packet based on the transmission medium of the distribution system (which is usually the Ethernet), and it is transmitted to the AP, which supports the STA2. Finally this packet is retransformed to 802.11 and transmitted to the STA2 through the AP. [1]

Finally, it must be noted that all the wireless stations use 48-bit MAC addresses, which make thinking of the wireless network as an extension of the wired network easier. [1]

4. Authentication and Association

The association implements the procedure of how a wireless client gets connected to the network through an AP. This operation is important because, without it, the wireless client is unable to transmit or receive a packet via the corresponding AP. Association is actually an IEEE 802.11 service that enables the mapping of a wireless station to the wired distribution system via an access point. When a client is associated, it is connected to the network and able to pass traffic through the access point to which it is associated.[1]

Authentication is the mechanism by which a client station announces itself by transmitting its identity to another client station. During the authentication procedure, the station tries to verify itself to the network. In the IEEE 802.11 standard, this process does not involve a great deal of checking. If the manager of the network decides that it is important, then every user or client of the network has the obligation to authenticate his identity before the association takes place. [1]

There are two ways of authentication in general. The client is either simply accepted under open-system authentication or challenged using a shared-secret key under shared-key authentication. These two ways are presented in summary below.

a. Open-System Authentication

Open-system authentication is the IEEE 802.11 default authentication method. Open-system authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second step in the sequence is the authentication result. If it is "successful," the client and the AP shall be mutually authenticated. [1]

According to [1], the following steps occur when two devices use Open-System Authentication:

- The station sends an authentication request to the access point.
- The access point authenticates the station.
- The station associates with the access point and joins the network.

This process is illustrated below in Figure 8.

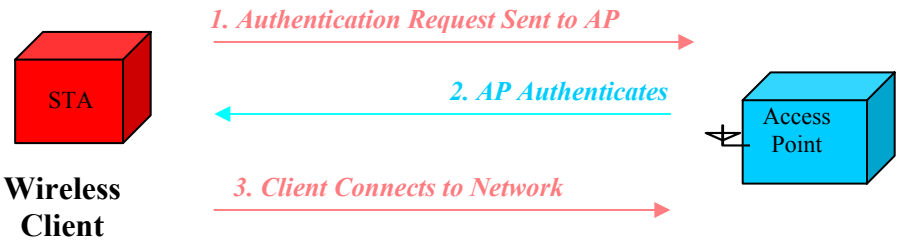

Figure 8. Open-System Authentication

If the privacy algorithm is used with open system authentication, then the client is allowed to associate, but the packets being passed between the access point and the station are encrypted. If both the access point and the station do not have the same encryption key, neither of them will understand what the other is saying, and the received packet is simply dropped. [1]

b. Shared-Key Authentication

The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. During the shared-key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudorandom number (PRN) sequence for the key/initial vector (IV) pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames. [1]

The 802.11 standard currently assumes that the shared secret key was delivered to the participating wireless clients by means of a more secure channel that is independent of IEEE 802.11 [1]. In practice, a user manually types this secret key for the wireless AP and the wireless client.

According to [1] shared-key authentication uses the following process:

- The authentication-initiating wireless client sends a frame consisting of an identity assertion and a request for authentication.
- The authenticating wireless node responds to the authentication-initiating wireless node with a challenge text.
- The authentication-initiating wireless node replies to the authenticating wireless node with the challenge text that is encrypted using Wired Equivalent Privacy (WEP) and an encryption key that is derived from the shared-key authentication secret.

- The authentication result is positive if the authenticating wireless node determines that the decrypted challenge text matches the challenge text originally sent in the second frame. The authenticating wireless node sends the authentication result.
- The station connects to the network.

This process is briefly presented in Figure 9 below.

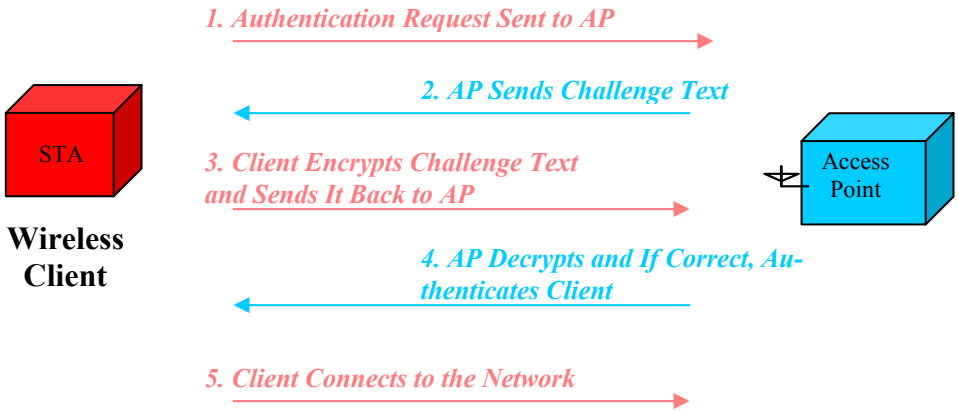

Figure 9. Shared-Key Authentication

If the decrypted text does not match the original challenge text (that is, if the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will not be able to communicate with either the 802.11 network or the Ethernet network. [1]

Note that, because both the challenge text and encrypted response are transmitted into free space, a hacker can collect them readily and then run an algorithm to recover the WEP key. This generally means that shared-key authentication is not secure enough. It is generally more secure to use WEP encryption with open-system authentication. [1]

5. Security Options

The IEEE 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN APs and NIC. The WEP algorithm is used to protect wireless communication from eavesdropping and "to provide data privacy to the

level of a wired network." [4] A secondary function of WEP is to prevent unauthorized access to a wireless network. This function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.

This security scheme, based on [4], uses the following five elements:

- A shared secret key, k. There is basically a set of four shared keys between all the clients of a service set and each time we use one of them. [4]
- WEP uses the RC4 stream cipher that was invented by Ron Rivest of RSA Data Security, Inc. (RSADSI) for encryption. [4]
- The third element is a 24-bit initialization vector (IV). An IV is a per-packet number that is transmitted without encryption.
- An encapsulated packet that is transmitted from the sender towards the receiver and contains the ciphertext and the IV.
- WEP also uses a Cyclic Redundancy Check (CRC) of the frame payload plaintext in its encapsulation. This CRC is computed over the whole data and is put next to it before the encryption process. The encryption process is then implemented to the whole data payload.

a. Description of WEP Implementation

The operation of WEP is very simple to describe. First, each client in the service set holds the shared key k via an unspecified mechanism.

Figure 10 below describes the whole transmission-reception procedure of a "WEP packet."

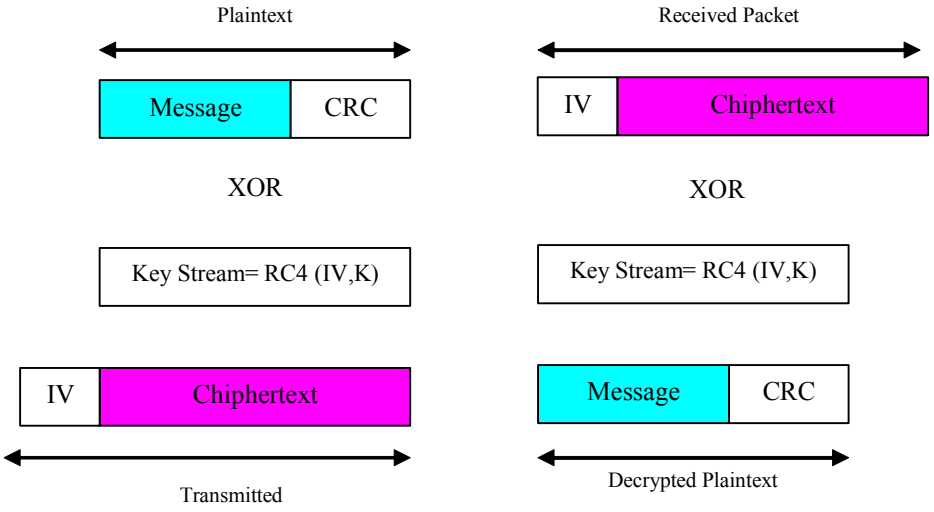

Figure 10. WEP Packet Procedure (After Ref. 5.)

When the transmitter wants to send an encrypted message via the "WEP mechanism," it first computes the CRC of that message. The message and the CRC form the plaintext. After that, the transmitter takes an IV, which is different each time, and appends it to the shard key k. Then, through the RC4 stream, the IV and the shared key are combined and they form a new key, the k_{new}. The length of the k_{new} is the same with the length of the plaintext. Finally the plaintext is "XORED" with the k_{new} and the result is the ciphertext. The IV is appended to the ciphertext and the transmitted message is formed. [4]

At the receiver end, to process a WEP packet, the opposite procedure is followed. The IV is extracted from the received packet and it combined with the shared key k in order to form the k_{new}. At last, the result of the XOR procedure between the received packet and the k_{new} is the decrypted plaintext. Finally the receiver verifies the CRC of the decrypted payload data to verify that the message was decrypted correctly.[4]

6. WEP "Improvements"

Although WEP is still used in many WLANs, it has proved to be not as "secured" as first thought. Several flaws have been discovered [4]. So enhancements were needed to address the WEP vulnerabilities that were uncovered. It has turned out that the WEP should be used only in cases in which we are not too concerned about having high security implementation, such as when we are sure that we are in a friendly environment during military operations. Secure communications is a great issue, not only in military operations but also in industrial and commercial operations. Thus the need of a "more secure mechanism" was immediate. [4]

a. Wi-Fi Protected Access (WPA): The Next Step

WPA tried to address the flaws in WEP, the original security mechanism for WLANs that has been in place since the IEEE 802.11 standard started to be implemented. A series of independent studies from various institutions showed that an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to a WLAN, even with the WEP enabled.

Although no security solution can claim to be "bullet-proof," WPA is, at least presently, a very secure mechanism in wireless communications. WPA is built on standards-based interoperable security enhancements. WPA not only provides strong data encryption to correct any WEP's weaknesses, it also adds user authentication, which was largely missing in WEP. WPA is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a and 802.11g. [6]

One of WEP's most important weaknesses is that the use of a static key. This key is entered manually on the AP and on all clients that communicate with the AP. It does not change unless it is manually re-entered on all devices. If one collects enough data he can threaten a WEP, without its size being an important issue. [4]

One major improvement over WEP is the Temporal Key Integrity Protocol (TKIP). This feature dynamically changes keys as the system is used. TKIP uses a kind of key hierarchy and implements a methodology that removes the predictability, which intruders relied upon to exploit the WEP key. [6]

Thus, the TKIP uses the 802.1x framework. The authentication server uses 802.1x and develops a specific key for each one transmission. Through TKIP this key is distributed to the both cooperating stations and it is used to generate a unique dynamic series of key at both the receiver (k_r) and the transmitter (k_t). Each pair of k_r and k_t can be used to encrypt and decrypt messages. TKIP's key hierarchy exchanges the WEP's single static key for "some 500 trillion possible keys that can be used on a given data packet." [6]

The CRC of the WEP mechanism is proved to be insecure. A hacker can change the message and update the message CRC without knowing the WEP key [4]. So an extreme mathematical function is implemented in WPA, namely the Message Integrity Check (MIC). Both the receiver and the transmitter compute and compare the results of the MIC verifying the integrity of the transmitting data. If the two results do not match, then a replay attack is assumed to have happened and that specific packet is rejected [6].

Even though these features are strong enough, the RC4 algorithm is still a vulnerable implementation. Thus, the WPA2 was developed. Its major improvement was

a new cipher scheme, the Advanced Encryption Standard (AES). AES has already been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). [6]

In Table 1 below we present the most important differences between the two security mechanisms, WEP and WPA.

WEP	WPA
Has been cracked several times	Not cracked yet, at least from what we know
Uses a static key	Uses dynamic session keys (TKIP)
Distribution of keys not specified	Distribution of keys is automatic (TKIP)
Authentication by WEP, which has several flaws	Authentication using 802.1x

Table 1. Improvements of WPA Compared to WEP (After Ref. 6.)

Finally, WPA can easily be installed as a software upgrade on most current Wi-Fi devices. APs require a software upgrade. Client workstations require a software upgrade to the network interface card and a possible software upgrade to the operating system. [6]

7. Beacon Packet

A beacon packet is actually a management kind of packet. This packet is periodically transmitted by the AP, and we have already mentioned some functions connected to it. Its basic purpose is to let all the stations know the existence of the network in its coverage area [1]. Also based on [1], the beacon packet contains various parameters of the network, informing the clients of:

- The time synchronization between the clients and the access point.
- The passing channel selection information.
- Informing clients of supported transmission rates.
- The DSSS and FHSS parameter sets.
- The capacity information and supported rates.
- The traffic Indication Map.
- The use of encryption mechanism.

8. Power Management Modes

Power-Saving Poll (PSP) mode, part of the 802.11 standard, is a feature that helps a wireless client to be in a "sleeping mode" without having to be on all the time. In that way it can preserve energy and battery life.[1]

All the stations and the APs are able to buffer temporarily the packets that are headed to stations that are in a sleeping period. So the stations are able to "wake up" periodically and receive the packets that are saved to the APs, or to transmit packets to the APs. [1]

A station that has just woken up may ask the AP to transmit all the packets that are saved for it with the transmission of a PS-Poll packet. When the AP receives such a packet, then it can either start transmitting packets to that station immediately, if there are any, or it can transmit an ACK packet immediately and transmit the saved packets at a later time. In the second case, the station must wait until it receives all its packets before it returns to a sleeping period again. [1]

9. Access to the Medium

In the 802.11 standard, the mechanism that is used for access to the medium is the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). There are two operation modes, a decentralized one, using the Distributed Coordination Function (DCF) and a centralized one, using the Point Coordination Function (PCF), which is actually an extension of the DCF. The PCF algorithm is executed only in APs, and therefore it can only be used in infrastructure networks. [1]

a. Access to the Medium Using the DCF Algorithm

The DCF algorithm, as already mentioned, is decentralized. Thus it can be used with any kind of wireless networks. This algorithm contains some basic steps that any station follows before transmitting a wireless packet [1]. These steps that are analytically referred to [1], are the following:

- Each station, before it tries to transmit a packet, checks if the wireless medium is busy.
- If the wireless medium is busy, then the station keeps checking periodically, waiting for free medium. If the medium is free, the station waits for a period of time, which depends on the kind of the transmitted packet, and

then it checks the medium again. The waiting time which is used is usually the DCF Interframe Space (DIFS). In the case that the station wants to transmit a packet CTS, an ACK packet or fragment of a larger packet, then the waiting time is the Short Interframe Spacing (SIFS). [1]

- If, in the optimum case, the medium is not busy, then the station transmits its packet. Then, if the medium is busy the station waits until the medium is free of packets for Interframe Space (IFS). In that time, the procedure of the binary exponential back-off commences, trying to implement the addition waiting period. A value of the contention window is chosen, and when this period ends, the station transmits its packet. [1]

If the transmission is unsuccessful then a collision has most probably taken place. In such a case, the station again chooses a new value from the contention window, which this time is longer than the previous one and tries to retransmit the packet. This procedure is repeated until a successive transmission takes place or the packet is rejected. [1]

This is a basic mechanism used so that a station can gain control of the medium. Of course, there are some other rules, which complete the above steps, and they depend on the specific situation or on the end of the previous transmission.

b. Access to the Medium Using the PCF Algorithm

The PCF algorithm is the alternative solution to the problem of how to access the medium. Its function is very similar to many schemes of access control, which are token based. This specific algorithm is not used so much for the commercial products and the various vendors do not have to support it since it is not a mandatory feature function of the 802.11 standard. It can be used only for infrastructure networks because it requires central control from an AP. [1]

The purpose of the PCF algorithm is to offer access to the medium without contention between the stations (contention-free (CF) medium access). It uses the structure of the DCF algorithm, plus an extra function. Its use needs the creation of contention-free periods. During the rest of the time the access is controlled by the DCF (contention periods). These periods are repeated successively and their duration each time is called the contention-free repetition interval. [1]

During the contention-free period the procedure of accessing the medium is controlled by the APs. In the beginning of this time period, the AP transmits a Beacon packet, which contains the maximum duration of the contention-free period. Then all the client stations set the Network Allocation Vector (NAV) to that maximum value not allowing the access by using the DCF for that period. [1]

When the AP takes over control of the medium, it transmits permission for transmission successively to each station through a polling packet (CF-poll). The reception of these polling packets needs to be confirmed by ACK by the stations. If a station does not transmit an ACK after receiving a polling packet, then the AP cooperates with the next station. All the participating stations, during the procedure of the association with the AP, get on a list, the polling list, so that the AP offers the transmission privilege during the contention-free period. We should notice that each polling packet allows the transmission of only one packet. [1]

The duration of the contention-free period must at least equal the period time needed for a maximum length packet to be transmitted and ACK. In the case when the contention period does not finish before the contention-free period has to start, then the contention-free period has a reduced duration. The AP that controls the PCF is able to stop the contention-free period for any reason. Finally, the stations want to take advantage of the contention-free period as much as possible. So they usually combine ACKs, polling and data into one packet, and we have complex packets, with many functions. For example, a station is able to combine the transfer of data with the acknowledge of the polling packet in a common packet and transmit it. The AP will receive it and is able to transmit a common packet of ACK of data to the transmitter and the data to the receiver station. [1]

10. Conclusions of the Architecture of the IEEE 802.11

In concluding the above discussion, it is obvious that the theoretical transmission data rates have nothing to do with the real effective data rate, which is called throughput. The overhead bits, which are necessary and valuable because of the whole IEEE wireless

structure, the retransmissions and the collisions decrease the time needed for a packet of data to be transferred. In the later chapters, measurements of the 802.11g signals and determination of the actual data throughput are presented.

C. 802.11G THE NEW STANDARD

Few technologies have received as much anticipation as 802.11g, the IEEE standard for WLAN, which operates in the 2.4-GHz band with a top data rate up to 54 Mbps. Currently, the two previous IEEE standards are the 802.11b in the 2.4-GHz Industrial-Scientific-Medical (ISM) band, which uses Complementary Code Keying (CCK) at the higher data rates, and the 802.11a in the 5-GHz Unlicensed National Information Infrastructure (U-NII)/ISM bands in the US, and license-free 5-GHz bands elsewhere, which uses Orthogonal Frequency Division Multiplexing (OFDM). The former offers data rates of 1, 2, 5.5 and 11 Mbps, while the latter is capable of supporting higher data rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. Standard IEEE 802.11g, formally approved in July of 2003, is drawing attention recently based on the use of all the above mentioned data rates and OFDM technology as employed in 802.11a, plus backward compatibility with 802.11b devices. [3]

1. 802.11g in Summary

In Table 2 below, we see channel numbers, the center frequency of each one of them as well as their bandwidth, as they are implemented in 802.11g standard. It is useful to note that the frequency spread of each channel equals 25 MHz. [3]

802.11g Radio Frequency Channels		
Channel	**Center Frequency**	**Frequency Spread**
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz

802.11g Radio Frequency Channels		
Channel	**Center Frequency**	**Frequency Spread**
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Table 2. Available Frequency Channels (After Ref. 3.)

The available channels supported by the wireless products in various countries are different. For example, channels 1 to 11 are supported in the U.S. and Canada, and channels 1 up to 13 are supported in Europe and Australia. [3]

Since the separation between the channels in neighboring wireless networks is 25 MHz, three different channels should be within our wireless network. It is recommended that we start using channel 1 and grow to use channels 6 and 11 when necessary, as these three channels do not overlap.

The IEEE 802.11g WLAN standard can be thought of as a combination of both the 802.11b and 802.11a standards. Like the 802.11b, 802.11g operates in the same 2.4-GHz band of the radio frequency spectrum that allows for license-free operation on a nearly worldwide basis. An important mandatory requirement of 802.11g is full backward compatibility with 802.11b. Like 802.11a, the 802.11g uses Orthogonal Frequency Division Multiplexing (OFDM) for transmitting data. OFDM is a more efficient means of transmission than Direct Sequence Spread Spectrum (DSSS) transmission, which is used by 802.11b. We should note at this point that all the above information are based on [3].

When coupled with various modulation types, 802.11g is capable of supporting much higher data rates than those of 802.11b. As noted in Table 3, 802.11g uses a com-

bination of OFDM and DSSS transmission to support a large set of data rates. This set of data rates is in fact all the data rates that are supported by both 802.11a and 802.11b. The 802.11g standard can be regarded as an improved version of 802.11b, providing all the functionality of, and backward compatibility with 802.11b, plus the higher performance associated with OFDM transmission. [3]

Data Rate (Mbps)	Transmission Type	Modulation Scheme
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK
12	OFDM	QPSK
11	DSSS	CCK/PBCC
9	OFDM	BPSK
6	OFDM	BPSK
5.5	DSSS	CCK/PBCC
2	DSSS	QPSK
1	DSSS	BPSK

Table 3. Data Rates and Modulation Methods (After Ref. 3.)

Table 4 summarizes the key differences between the three WLAN systems.

	802.11a	802.11b	802.11g
Operating frequencies	5-GHz U-NII/ISM Bands	2.4-GHz ISM Band	2.4-GHz ISM Band
Modulation techniques	OFDM	Barker Code/ CCK/ PBCC	Barker Code/ CCK/ OFDM/ PBCC
Data Rates (Mbps)	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	1, 2, 5.5, 11 6, 9, 12, 18, 24, 36, 48, 54
Slot time	9 μs	20 μs	20 μs 9 μs (optional)
Preamble	OFDM	Long/ Short (optional)	OFDM/Long/Short

Table 4. Key Differences of the Three Most Popular Standards (After Refs. 2,3,7)

2. Differences 802.11g from 802.11a

In theory, both 802.11g and 802.11a use almost the same PHY specification and, therefore, should have similar throughput performance. In reality, 802.11g throughput performance will be significantly different from 802.11a for the following reasons:

- 802.11g mandates the use of a 20-μs slot time in order to be compatible with the current 802.11b devices. The use of a 9-μs slot time as is used in 802.11a is used only when the WLAN contains only 802.11g users. [2,3]
- 802.11g shares the same 2.4-GHz spectrum as 802.11b. When both 802.11g and 802.11b devices are present, the performance impact may be significant if no coordination is employed between 802.11b and 802.11g users. [2,3,7]
- Even without considering co-existence with 802.11b devices, it is true that 802.11g devices will not have equivalent performance to 802.11a devices simply because of the frequency band in which they operate. This section describes the effects of propagation and channel availability, and how they are different in the cases of 802.11a and 802.11g. Frequency-dependent propagation loss favors 802.11g, that is, free space path loss is greater at 5 GHz than at 2.4 GHz. However, the prevalence of non-WLAN devices in the 2.4 GHz ISM band, e.g., Bluetooth devices, cordless phones, microwave ovens, etc. raises the probability of 802.11g devices encountering interference harmful to WLANs. [2,3]
- There are fewer available channels in the 2.4 GHz band than in the 5 GHz bands. For example, *only three non-overlapping channels exist in the US 2.4 GHz ISM band compared with 13 available channels in 5 GHz U-NII band.* (The number of channels is even larger in other regulatory domains and is likely to increase to more than 20 channels in the US.) Unlike in the home application, frequency reuse is necessary for enterprise/public space use to support coverage and capacity requirements. Co-channel interference due to frequency reuse is more likely when fewer channels are available. [2,3]

3. Compatibility with 802.11b

As noted above, 802.11g operates in the 2.4-GHz frequency band, as the 802.11b. But this feature is not by itself enough for the 802.11g to be compatible with legacy 802.11b. The 802.11 networks use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), a media access method similar to that of shared Ethernet. Also, 802.11b devices, which share the same 2.4 GHz band as 802.11g, have no means of detecting OFDM transmissions. Although 802.11b devices can sense “noise” in the 2.4-

GHz band via their Clear Channel Assessment (CCA) capabilities, they cannot decode any data, management, or control packets sent via OFDM. Given this, the 802.11g standard includes protection mechanisms to provide for coexistence and backward compatibility. [2,7]

When 802.11b clients are associated to an 802.11g access point, the access point turns on a protection mechanism called Request to Send/Clear to Send (RTS/CTS). Originally a mechanism for addressing the "hidden node problem," RTS/CTS adds a degree of determinism to the otherwise multiple access network. When RTS/CTS is invoked, clients must first request access to the medium from the access point with a RTS message. Until the access point replies to the client with a CTS message, the client refrains from accessing the medium and transmitting its data packets. When received by clients other than the one that sent the original RTS, the CTS command is interpreted as a "do not send" command, causing them to refrain from accessing the medium. It is obvious that this mechanism precludes 802.11b clients from transmitting simultaneously with an 802.11g client, thereby avoiding collisions that decrease throughput due to retries. One can see that this additional RTS/CTS process adds a significant amount of protocol overhead that also results in a decrease in network throughput. [2,7]

D. PATH LOSS MODELS

1. Free Space Path Loss Model

One of the most obvious differences between 802.11g devices and 802.11a devices is that they operate in different frequency bands. Because the size of the antennas used to transmit and receive signals depends on the frequency, for antennas with similar characteristics there is a frequency dependent effect on the reduction in signal strength as measured by two antennas. This effect is commonly referred to as frequency dependent path loss. [8]

According to [8, p.107], the propagation model which best describes the microwaves radio signals is the Free Space Propagation Model. This model is valid only when there is a clear Line of Sight (LOS) between the transmitter and the receiver. The free space power $P_r(d)$ which is received by a receiver antenna located at d meters away from a transmitting antenna is given by the equation

$$\mathrm{P}_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}, \tag{2.1}$$

where P_t is the transmitted power; G_t and G_r are the gains of transmitter and receiver antennas, respectively; λ is the wavelength of the signal wave measured in meters and L is the system loss factor not related to the propagation.

Depending on the free space equation, the path loss, which represents the signal attenuation as a positive quantity measured in dB, is the difference in dBs between the transmitted power and the received power. If we assume that both the antenna gains are equal to unity, then the path loss is given by

$$\mathrm{PL[dB]} = -10\log\left[\frac{\lambda^2}{(4\pi)^2 d^2}\right], \tag{2.2}$$

where the minus sign shows that we have to subtract this quantity from the transmitted power (in dBs) in order to compute the received power (in dBs).

An alternative form of the formula in (2.2) is

$$\mathrm{PL[dB]} = -20\log\lambda + 20\log(4\pi) + 20\log d. \tag{2.3}$$

If we assume that the antenna gains are not equal to unity, which is the case in most of the real implementations, then the path loss is given by

$$\mathrm{PL[dB]} = -10\log\left[\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2}\right], \tag{2.4}$$

where we accept, of course, that the free space model is valid.

According to (2.2) the path loss varies with the wavelength λ and the distance d between the source and the receiver. This means that, keeping the distance constant, the 802.11g, with its basic frequency being equal to $2.4\,\mathrm{GHz}$, will obviously have less path loss than the 802.11a, with its basic frequency being equal to $5\,\mathrm{GHz}$. In Figure 11 we can see the Path Loss versus the distance in meters for the 2.4-GHz and 5-GHz case, assuming unity antenna gains.

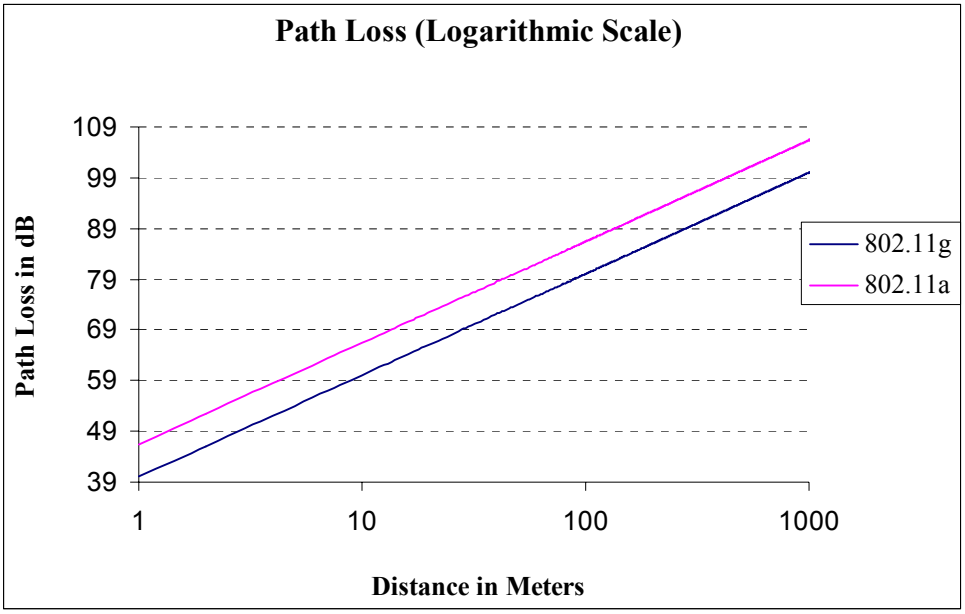

Figure 11. Path Loss (Free Space Equation)

As this figure shows, in the simple free space model there is approximately a 6 dB difference between propagation at $2.4\,\text{GHz}$ and propagation at $5\,\text{GHz}$, since

$$20\log\left(f_2 = 5\,\text{GHz}\right) - 20\log\left(f_1 = 2.4\,\text{GHz}\right) = 6.4\,\text{dB}.$$

In deployments such as military operations, in which signal range is the most important factor, this effect favors the 802.11g devices since, in principle, the signals from those devices will propagate further with less loss.

2. Two-Ray Model

In the microwave signal propagation, the heights of the transmitting and receiving antennas are very important factors. This is implemented by the two-ray Ground Reflection Model. This model is based on geometric optics and considers both the direct path and a ground reflected propagation path between the transmitter and the receiver. It has also been proven to be reasonably accurate for computing and predicting the large scale signal strength over distances of several kilometers for the wireless radio spectrum, provided that a LOS between the transmitter and receiver is maintained.

According to [8, pp. 120] the two-ray model is valid for distances d from the transmitter which satisfy the equation

$$d > \frac{20 h_t h_r}{\lambda}, \tag{2.5}$$

where d is measured in meters, h_t and h_r are the heights of the transmitting and the receiving antennas, respectively, all in meters. It is very interesting that this distance metric has nothing to do with the antenna gains.

Thus, according to the two-ray model theory, the received power is given by

$$\mathrm{P}_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4}, \tag{2.6}$$

where we assume that the antenna gains are the same for the direct and reflected path, and are not equal to unity. Therefore, the path loss formula based on the two ray model is

$$\mathrm{PL[dB]} = 40 \log d - (10 \log G_t + 10 \log G_r + 20 \log h_t + 20 \log h_r). \tag{2.7}$$

As we can see from Equation (2.6), the received power falls off with distance raised to the fourth power or, from a logarithmic view, at a rate of $40\,\mathrm{dB}$ per decade according to (2.7). In this case, the loss is greater than in the free-space case. Finally it is very important to note that the received power and the path loss become independent of frequency.

Suppose we install an 802.11g transmitting wireless antenna with unity gain in a position of height $h_t = 40\,\mathrm{m}$, and a unity gain receiving antenna, which is in a position with height $h_r = 1.2\,\mathrm{m}$. Then, according to (2.5) the two-ray model is valid for distances greater than the distance $d = 7.68\,\mathrm{km}$.

In Figure 12, we can see the path loss (in dB) versus distance d (in meters), in a logarithmic scale, for both the two-ray and free-space loss models for distances greater than 1000m. As mentioned above, beyond the distance of the 7.68 km the two-ray model can be used to compute the theoretical signal path loss.

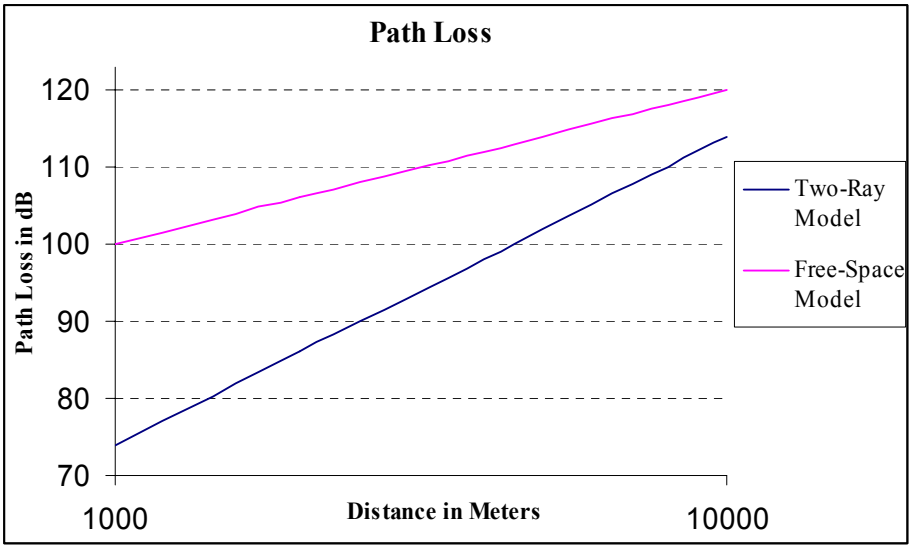

Figure 12. Two-Ray Model Path Loss

This is a specific example, where we are able to view the way the Path Loss increases while the Transmitter-Receiver distance increases, for both cases (free-space and two-ray model). It is obvious that the increase for the first case is greater.

E. DISTANCE DETERMINATION

In this research, the distance between the AP (transmitter) and the client (receiver) is determined by a GPS receiver named Etrex by Garmin, operated in navigation mode. However, as an extra check, we also used the coordinates provided for each location.

According to [9] the applicable formula for computing the separation distance between two positions, *S,* is the following:

$$S[\text{miles}] = \sqrt{\left(\Delta_{\text{LAT}} \times 69.2\right)^2 + \left(\Delta_{\text{LONG}} \times 55.6\right)^2}\ , \tag{2.8}$$

where Δ_{LAT} is the difference of the latitudes between the two positions, and Δ_{LONG} is the difference of the longitudes between the two positions.

To convert the separation to meters, we have to multiply the result by 1609.27 $(1\,\text{mile} = 1609.27\,\text{m})$,

$$S[\text{m}] = \sqrt{\left(\Delta_{\text{LAT}} \times 69.2\right)^2 + \left(\Delta_{\text{LONG}} \times 55.6\right)^2} \times 1609.27. \tag{2.9}$$

F. SUMMARY

The latest IEEE standard, the 802.11g, seems to be an effective way of consuming a high-transmission rate wireless network. It offers theoretical transmission rates of up to 54 Mbps and, compared to 802.11a, supports longer effective transmission ranges. The theoretical models that were presented will be used as a metric to the following chapters in order to evaluate some of the potential components of the prototype system.

The next chapter is devoted to the development of the prototype system that was able to process and analyze wireless 802.11g signals. It will show the procedure choosing the components of that system based on previous experience and on extensive experimental measurements.

III. MODELING THE PROTOTYPE SYSTEM

A. SUMMARY REQUIREMENT OF THE PROTOTYPE SYSTEM

The basic requirement of the prototype system is the ability to process WLAN packets and signals. That means it is able to capture, detect, analyze, and decode data, to monitor the traffic in our own network, and to detect other wireless networks that operate in close distances. Finally, it should be capable of detecting possible vulnerabilities of our WLAN. The following list summarizes the requirements we have set for our prototype system (not in order of importance):

- Software that is relatively easy to use and easy for a user to understand the analysis of its results. It also has to operate in a user-friendly environment, basically in the Windows OS environment.
- An ability to capture, analyze, decode and display 802.11g packets in real-time.
- Software and hardware with a relatively low cost that have been previously tested in various applications.
- Portability with high mobility and a large display screen.
- High sensitivity in acquiring WLAN signals and packets in an open area environment at long ranges.
- High storage capacity and processing power for our captured database.

B. SOFTWARE REQUIREMENT

The basic and most important tool that we need is suitable software that can be used as a packet sniffer and as a protocol analyzer. By using this tool properly, we can capture 802.11g packets and analyze the traffic of our network.

Generally, a protocol analyzer is a useful management tool that captures packets and monitors the traffic of a network. Its main purpose is to ensure that a specific network operates properly. Most of the time, protocol analyzers are used as test and planning tools, but we implement them only for troubleshooting and when we try to maintain the network.

There are several very simple packet sniffers/protocol analyzers, which can be downloaded from the Internet, generally without cost. These tools can be used by hackers, either amateurs or professionals, who operate them in order to explore and map a

specific region of interest for unsecured access points and networks. In order to deal with such problems as efficiently as possible, more complex and professional tools have been developed. Therefore, we use these advanced protocol analyzers to detect rogue access points, to assess possible security vulnerabilities and to monitor the traffic of our network.

1. Available WLAN Protocol Analyzers

As already mentioned, several available protocol analyzers can be used for capturing packets. Some of them are simple implementations, which operate on a laptop under an OS of Windows or MAC or Linux and are able to log onto a network automatically as soon as they detect an available one. Of course, there are also some other more advanced and complex implementations, which not only capture, decode and analyze 802.11g packets, but also have great potential and ability for detecting and analyzing IPs and implementing various types of packet filtering.

For this thesis, we needed an 802.11g WLAN protocol analyzer. We should note that in order to meet our system specifications, we built a laptop-based system instead of a Personal Digital Assistant (PDA) or any other handheld device-based system. The reason is that, although the laptop-case is not superior regarding mobility and portability, when we combine the mobility and display of data, then it is obvious that the laptop-based system is superior to all the other cases.

In Table 5 [9], we present the most important protocol analyzers.

Program	Vendor	OS Platforms	802.11 Type	NIC Required	Layers
Sniffer Wireless	Network Associates www.sniffer.com	Win 98, NT 4, 2000, XP	b or a	Proxim, Cisco, Symbol, Agere	2 to 7
AiroPeek NX	WildPackets www.wildpackets.com	Win 2000, XP	b, a and g	Any Intersil- or Atheros-based	2 to 7
LAN Planner	Wireless Valley Communications www.wirelessvalley.com	Win 98, NT 4, 2000, XP	b, a and g	Cisco Aironet	2,3
Observer	Network Instruments www.networkinstruments.com	Win 98, NT 4, 2000, XP	b, a and g	Cisco Aironet, Proxim Skyline	2 to 7
Air Magnet Laptop	AirMagnet www.airmagnet.com	Win 98, NT 4, 2000, XP	b, a and g	Supplied PC or CF+ Card	2 to 4

Table 5. Software-Based Wi-Fi Protocol Analyzers for Laptops. (After Ref. 9.)

As we see from the tools above, the AiroPeek NX from WildPackets, the Sniffer Wireless from Network Associates and the Observer from Network Instruments have the potential to perform analysis for Open System Interconnection (OSI) layers 2 to 7 and have the advantage of cooperating with commercial 802.11 Network Interface Cards (NIC).

It is interesting to note that the software candidates for the prototype system are similar to those referred to in prior theses by Currier [10] and Goh [9]. These theses evaluated both earlier and later versions of the first two protocol analyzers of Table 5, the Sniffer and the AiroPeek. Currier recommended the AiroPeek 1.1012 over the Sniffer Pro 4.6 based on its "sufficient capture capabilities, significant cost savings, and easy-to-use filtering capability," [10] and Goh mentioned that the AiroPeek NX is better "in terms of cost." [9]

Since the Sniffer Wireless is not able to support 802.11g signals, we cannot use it for this research. So our choice was between the AiroPeek NX and the Observer. In terms of cost, as of June 2004, the Observer costs $3,600 for a yearly subscription license [11] while the AiroPeek NX costs $3,500 for a 12-month license and maintenance contract [12]. The difference of cost is not significant. The fact that AiroPeek NX has already proved to be efficient enough in both 802.11a and 802.11b wireless signals with extraordinary capabilities is a very important factor. Therefore, because of this previous experience, the AiroPeek NX was the selected protocol analyzer for our prototype system.

a. Summary Review of AiroPeek NX

The AiroPeek is a software tool used as network analyzer in wireless LANs for monitoring the traffic in a network. It supports all three standards of IEEE 802.11a, b and g and helps a network administrator or a network expert analyze what is happening in a WLAN. A basic drawback is that it cooperates with specific wireless NIC in order to capture packets, while its greatest advantage is that it is very easy to install and to understand and analyze its results. It is actually a packet sniffer, letting the capturing device work in a "promiscuous mode" and receive every packet that is transmitted inside the network, regardless of the packet address. [12]

According to [12] the AiroPeek NX offers the following advanced capabilities:

- Full packet decoding of 802.11a, 802.11b, and 802.11g standards.
- Scanning for available networks by channels or by BSSID.
- Displaying data rate, channel and signal strength.
- WEP decryption, both on-the-fly and offline and packet decoding.
- Implementing packet filtering.

For example, in Figure 13 device A transmits a packet towards the device C. That means that the specific packet carries the header of the device C. All the devices that are within range receive that packet (devices B, C, D and E). As expected, device C receives and processes it and also transmits an ACK packet. Devices B and E disregard that packet and device D accepts it without transmitting any ACK packet.

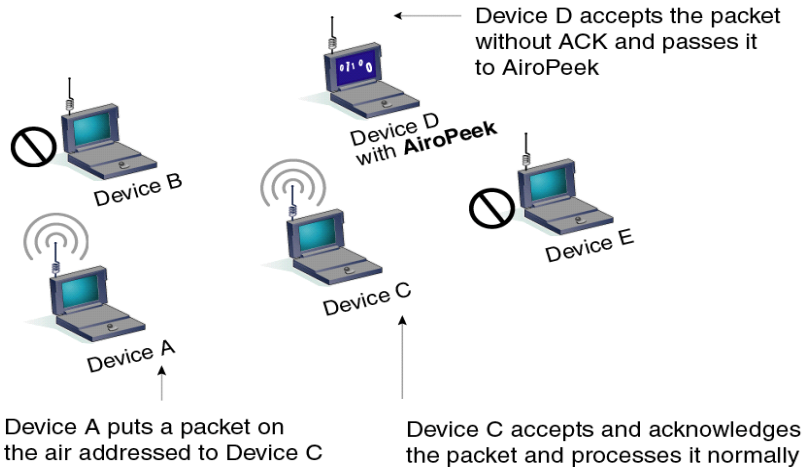

Figure 13. AiroPeek Captures Any Packet on the Air. (From Ref. 12.)

C. SELECTION OF HARDWARE

Based on the established characteristics and requirements, our prototype system was laptop-based, with the ability to log on, detect and analyze 802.11g signals, using a commercial 802.11g-compliant wireless card. In this section we present the selected parts of our system hardware.

1. Laptop: The Basis of the System

The most important considerations for selecting a laptop are the processing power, the storage capacity, and the capability of displaying the data and the results. This third requirement was not considered very important at the beginning of this research, but eventually it proved to be very important, since monitoring the traffic of the network in a real time basis was desirable.

For this experimental work, we used a laptop platform, the Dell Latitude C840. Its characteristics are listed in Table 6. Under the low cost consideration, without losing critical advantages of a laptop, this choice seemed to be very effective.

System Configuration	
Computer Processor	Intel Pentium 4
Operating System	Windows XP

System Configuration	
Display	UXGA 15", 1600 x 1200 pixels
RAM	512 MB
Hard-disk	20 GB
Secondary Storage	CD Read/Write Drive

Table 6. Dell Latitude C840 Configuration

2. Available Hardware for 802.11g Reception

During the research we tested three commercial 802.11g cards from different vendors in order to decide which one was more suitable for our prototype system. First we tested the Linksys WPC54G. Then we made experiments using the Proxim Orinoco GOLD 11a/b/g ComboCard (8480-WD) and, finally, we tested the D-Link AirPlus Xtre-meG DWL-650 Wireless Cardbus Adapter. During this first part, we used the same AP for cooperating with these three wireless cards. Since we wanted to compare these three available wireless cards, we tested them in the same environment. In the following we provide all the available characteristics and briefly describe the receivers/wireless cards and the AP we used.

a. Linksys WPC54G Card

The Linksys WPC54G PC Card is an 802.11g wireless card that was developed for home and office applications. The WPC54G has a fixed (integrated) antenna that is not removable. Based on the specifications [13], it has a new antenna that provides greater ranges and Linksys claims that the WPC54G has increased sensitivity that helps filter out interference and "noise" to keep the 802.11g signal clear. Linksys also claims that the WPC54G, which is shown in Figure 14 below, incorporated improved error correction in its chipset to keep it "operating at higher transmission rates for longer distances" [13].

Figure 14. Linksys Instant Wireless PC Card (From Ref. 13.)

It supports data rates up to 54 Mbps, and it can transmit in all eleven channels deployed for the 802.11g in USA. It uses OFDM modulation and supports the use of WEP, both 64-bit and 128-bit. It contains an internal omni-directional antenna and it operates only under the Windows XP environment. [13]

The WPC54G also has a feature known as integrated hardware power management. This feature varies its transmit power to conserve the battery life of the laptop. For the purpose of this thesis, the transmit power was always set to the maximum for all experiments.

b. Proxim ORiNOCO GOLD 11a/b/g ComboCard Gold

The ORiNOCO 11a/b/g ComboCard is produced by the Proxim to implement secure connections to 802.11b, 802.11a and 802.11g networks using only one wireless card. The ORiNOCO ComboCard also has an integrated antenna that is not removable. Like WPC54G, the 802.11g portion of the ORiNOCO ComboCard (Gold version) can operate on all 11 channels, including, of course, the three non-overlapping channels (1, 6, and 11) in frequencies 2.412 GHz, 2.437 GHz and 2.462 GHz, respectively. It is capable of delivering up to 54 Mbps under the "g-only" mode. The ORiNOCO ComboCard (Gold version) is also capable of enhancing security features using WEP of 64-bit and 128-bit. It is illustrated in Figure 15. [14]

Figure 15. ORiNOCO 11a/b/g ComboCard Gold (From Ref. 14.)

Based on the specifications [14], the ORiNOCO ComboCard (Gold version) has a transmit power of 60 mW (+17.8 dBm) in 802.11g mode. Like the Linksys card, its receive sensitivity is not stated. [14]

The ORiNOCO ComboCard (Gold version) also has a transmitter power control feature but as already mentioned, the transmit power was always set to the maximum.

c. D-Link AirPlus XtremeG DWL-650 Wireless Cardbus Adapter

The D-Link AirPlus XtremeG DWL-650 WLAN client adapter is an 802.11g compliant Cardbus adapter that operates in the 2.4 GHz on all 11 available channels. It is shown in Figure 16 and it offers a maximum data rate of 54 Mbps. Like all other 802.11g cards, it incorporates an integrated, non-removable antenna. [15]

Figure 16. D-Link AirPlus XtremeG DWL-650 Wireless Adapter (From Ref. 15.)

Based on the D-Link datasheet [15], the DWL-650 can achieve wireless speeds up to 108 Mbps in a pure D-Link 11g environment through the use of new wireless techniques such as Packet Bursting, FastFrame, Compression and Encryption, and Turbo mode. It also supports infrastructure networks via an access point and peer-to-peer communication in ad-hoc mode and provides a measure of security for the information transmitted over a wireless network with high data encryption at 64-, 128-, and 152-bit WEP. The wireless transmitting power is equal to 15 dBm, with an accuracy of 2 dBm. [15]

D-Link offers a very detailed receiver sensitivity information for the AirPlus XtremeG DWL-650 according to [15]. It is shown in Table 7.

Receiving Sensitivity (Typical)			
Data Rate	**Sensitivity**	**Modulation Type**	**Packet Error Rate (PER)**
54 Mbps	−68 dBm	OFDM	10%
48 Mbps	−68 dBm	OFDM	10%
36 Mbps	−75 dBm	OFDM	10%
24 Mbps	−79 dBm	OFDM	10%
18 Mbps	−82 dBm	OFDM	10%
12 Mbps	−84 dBm	OFDM	10%
11 Mbps	−82 dBm	CCK	8%
9 Mbps	−87 dBm	OFDM	10%
6 Mbps	−88 dBm	OFDM	10%
5.5 Mbps	−85 dBm	CCK	8%
2 Mbps	−86 dBm	QPSK	8%
1 Mbps	−89 dBm	BPSK	8%

Table 7. D-Link AirPlus XtremeG DWL-650 (After Ref. 15.)

Moreover, the DWL-650 wireless card is theoretically capable of capturing wireless signals up to 400 m, for outdoor cases. [15]

d. AP- Linksys WAP54G

During the sensitivity experiment, we used the AP of Linksys WAP54G shown in Figure 18, cooperating with all the above-mentioned wireless cards.

Figure 17. AP- Linksys WAP54G (From Ref. 16.)

This AP has a transmitted power of 15 dBm and its antenna gain is 5 dB. It also supports security features, as it uses WEP of 64 or 128 bits, depending on the settings, and it also supports data rates up to 54 Mbps. The receiving sensitivity is -80 dBm for 11 Mbps and -65 dBm for the 54 Mbps. It uses the following types of modulation: CCK, DQPSK, DBPSK and OFDM. [16]

This AP can be installed and set up easily. This can be done not only using the corresponding installation CD-rom but also through its web page, while the client and the AP are connected through the wireless network. The set-up page is shown in Figure 18.

Figure 18. AP- Linksys WAP54G Set-Up Page

We can select the type of the network (mixed or "g-only"), the subnet mask, the IP and the Gateway address. We can also select the number of the channel in which the AP transmits as it operates in all 11 available channels for USA [16]. For our research purpose, we used channel number six, which means that the AP operated at a frequency of 2.437 GHz, in the "g-only" mode.

3. Sensitivity Measurements (LOS)

It is worth pointing out that while the receiver sensitivities for the D-Link AirPlus XtremeG DWL-650 are available, those of Orinoco ComboCard and Linksys WPC54G are not. Thus, an experimental methodology was used to determine which of the three available 802.11g wireless cards performed best for the prototype system.

a. Test Set-up

To test the receive performances, the above mentioned AP was used as a source of 802.11g packets. The AP was set up to transmit the beacon continuously. The

beacon frames, which are 75 bytes in length, were transmitted at 1 Mbps (the lowest available rate) on channel 6. Channel 6 was arbitrarily chosen because it is one of the three non-overlapping channels of the 802.11g. Also, based on Equation (2.2), the free-space propagation loss is not affected much even if another channel (with different wavelength) within the band is selected. The AP was set for open authentication with no WEP encryption, since we assumed that the sensitivity has nothing to do with encryption.

The AP was set on a platform mounted on a hand-supported stick on the Monterey beach at a height of 305 cm without any objects positioned in the vicinity. All three 802.11g-compliant cards were then used with the AiroPeek NX software in the prototype system to capture the beacon frames transmitted from the WAP54G. The prototype system was stationed at various distances away from the location of the AP, always preserving a clear LOS. Ten to twenty thousand of beacon packets were captured for each measurement.

To determine the exact location of each of the measurement points, we used the Garmin *e*trex handheld GPS receiver. According to [17], this device has an accuracy of 15 to 20 ft. Using the navigation mode, the distances were marked out along the LOS path from the AP position. As an extra check, the location coordinates of the measurement points given by the GPS device were also noted. The measurement environment is shown in Figure 19.

Figure 19. LOS Measurement Environment

The coordinates provided by the GPS receiver at various measuring positions are presented in Table 8. In the third column, the calculated separation distances using Equation (2.9) are also listed. These calculations prove that the accuracy of the GPS device is acceptable.

Location Marked by GPS Navigation Mode	Coordinates of Measurement Positions	Distance Calculated from Equation (2.9)
AP	$N36^{\circ}36'06.2"\ W121^{\circ}53'23.1"$	-
75 m	$N36^{\circ}36'06"\ W121^{\circ}53'20.1"$	74.82 m
110 m	$N36^{\circ}36'05.45"\ W121^{\circ}53'18.8"$	109.3 m
140 m	$N36^{\circ}36'04.9"\ W121^{\circ}53'17.5"$	144.87 m
210 m	$N36^{\circ}36'03.8"\ W121^{\circ}53'14.9"$	216.91 m
245 m	$N36^{\circ}36'03.7"\ W121^{\circ}53'13.6"$	248.95 m
320 m	$N36^{\circ}36'02.6"\ W121^{\circ}53'11.0"$	321 m
395 m	$N36^{\circ}36'11.5"\ W121^{\circ}53'08.4"$	393.2 m

Table 8. Separation Distances

At each location, about 15,000 packets of beacons were captured for each measurement. Ten sets of measurements were performed for each of the 802.11g cards at each distance. For all the measurements, packet filtering was used so that the 802.11g card captured only beacon packets transmitted by the Linksys AP.

b. Theoretical Results

The theoretical Path Loss at various distances can be calculated using Equation (2.3), as mentioned in Chapter II. As stated earlier, the AP transmits at a power of $+15\,\text{dBm}$. Substituting the frequency of 2.437 GHz and the various distances into Equation (2.3), the expected signal Path Loss assuming a LOS path with no multipath effects is tabulated in Table 9.

Location	Theoretical Free-Space Path Loss
75 m	82.5 dB
110 m	85.9 dB
140 m	88 dB
210 m	91.5 dB
245 m	92.9 dB
320 m	95.1 dB
395 m	97 dB

Table 9. Theoretical Free-Space Signal Path Loss

We should note that although the measurement environment did provide a direct LOS path between the AP and the prototype system, multipath effects were still expected. Thus, the values in Table 9 could be used only as a comparison metric of the expected signal Path Loss at the various measurement points. Experimental measurements were expected to deviate from the theoretical values.

c. Measurement Results and Analyses

For each distance, the average Path Loss, as detected by the 802.11g wireless cards under test, the number of packets captured, and the Packet Error Rate (PER) were recorded. Note that the PER was referred to the beacon packets and not to the entire wireless 802.11g network. The measurement results for Linksys WPC54G are tabulated in Table 10.

Distance	Number of Captures	Average Signal Path Loss	Number of Captured Packets	Packet Error Rate (%)
75 m	15	79.25 dB	20,000	0.193
110 m	15	85.2083 dB	25,000	0.332
140 m	15	91.1665 dB	18,000	1.91
210 m	15	93.8488 dB	15,000	2.44
245 m	15	96.531 dB	18,000	4.49
320 m	15	100.513 dB	25,000	11.88
395 m	15	101.665 dB	10,000	12.31

Table 10. Measurement Results for Linksys WPC54G

From these measurements, it was observed that the signal Path Loss for the Linksys WPC54G showed a sudden increase at both the110 m and 245 m points. This is likely due to multipath effects mentioned earlier.

From the captured files, it was also observed that the percentage of the CRC packet errors started to become significantly large at a path loss of about 96 dB, that is, after the 245-meter point.

Comparing the measured signal Path Loss for the Linksys WPC54G against the theoretical values in Table 9, it was noted that the values reported by the WPC54G were very close to the theoretical values (Free-Space equation) for an approximate distance of 110 m. For distances beyond that point, the signal path loss did not follow the Free-Space model. That is, it did not vary based on the d^2, where d is the distance from the source (AP). So, we tried to calculate a new path loss exponent for d that would allow the model to approximate the measured signal path loss values for distances greater than 110 m from the AP. Based on the Equation (2.4), we tried several values for the exponent of d. This trial-and-error method resulted to the following path loss equation

$$\mathrm{PL[dB]} = -10\log\left[\frac{G_t G_r \lambda^2}{(4\pi)^2 d^{2.2}}\right], \tag{3.1}$$

The computed values of Equation (3.1) for various distances used in the experiment are tabulated in Table 11.

Location	Path Loss Based on Equation (3.1)
75 m	86.3 dB
110 m	90 dB
140 m	92.3 dB
210 m	96.1 dB
245 m	97.6 dB
320 m	101.2 dB
395 m	97.2 dB

Table 11. Calculated Values Based on Equation (3.1)

In Figure 20 we see the Path Loss measured values, the theoretical Free-Space equation values and the path loss values based on Equation (3.1).

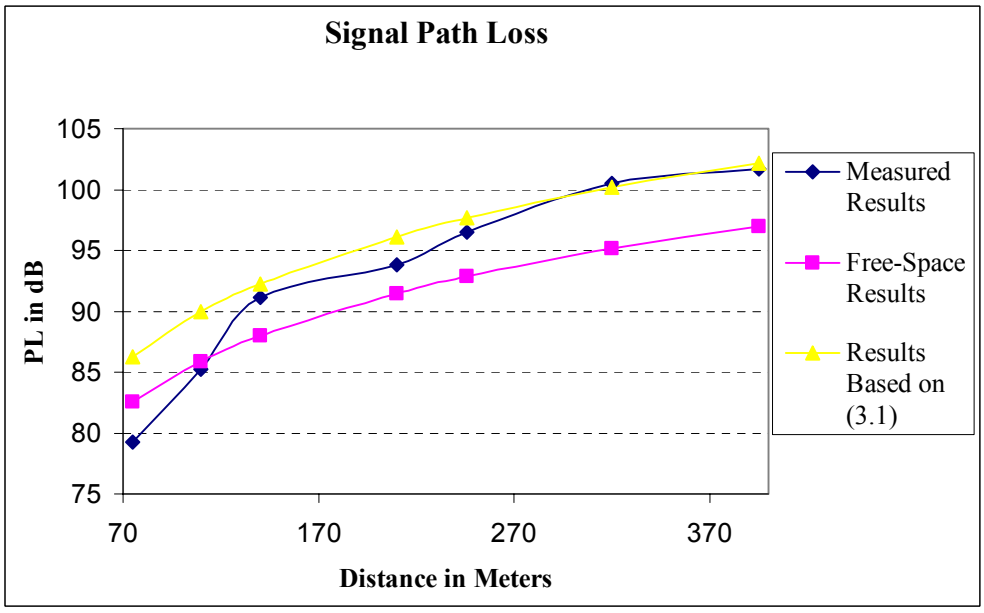

Figure 20. Linksys Signal Path Loss Results

Figure 20 shows that at distances greater than the 110 m, the signal path loss no longer follows the Free-Space equation. This is due to the multipath effects, and it is closer to the $d^{2.2}$ values computed by Equation (3.1).

At this point we should note that all the graphs were created with the help of the Microsoft Excel. We input the measured and the calculated data values for each distance and Excel created the corresponding graph connecting these data points with a trend line that is a sixth order polynomial.

Figure 21 illustrates the PER for the Linksys case measured in percent.

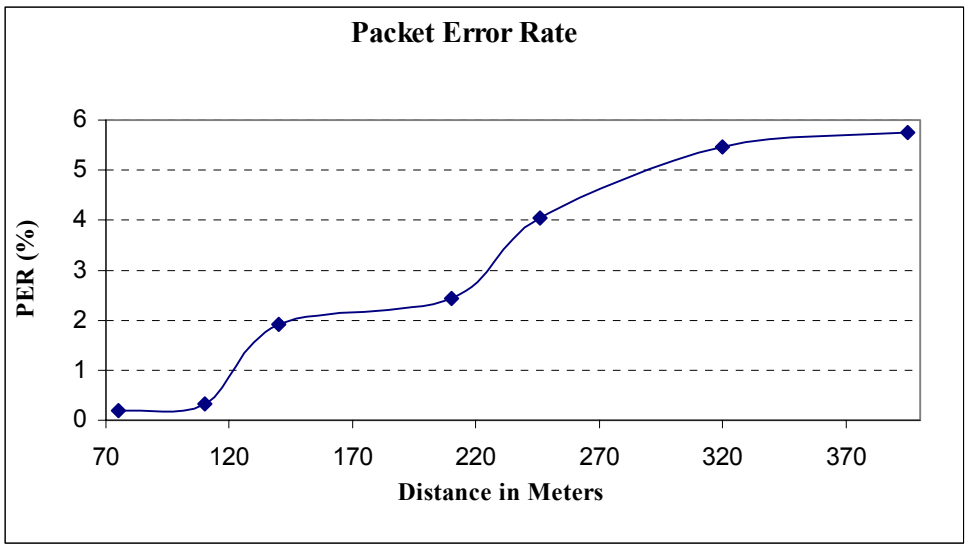

Figure 21. Measured Linksys Beacon PER

As we expected, the PER was very low since the transmission rate was the lowest possible (1 Mbps). Note the significant increase in the error rate after the distance of 110 m and after the distance of 245 m, which of course has to do with the increase of the signal path loss we noted above.

The measurement results for the ORiNOCO ComboCard are tabulated in Table 12. Again similar results due to the multipath effect at the 110- and 245-meter point were observed. When we compare the signal Path Loss measured result for the

ORiNOCO ComboCard of the Table 12 against the theoretical values in Table 9, our conclusions are the same as with the Linksys case.

Distance	Number of Captures	Average Signal Path Loss	Average Number of Captured Packets	Number of Error Packets (%)
75 m	15	78.34 dB	20,000	0.021
110 m	15	86.822 dB	25,000	0.044
140 m	15	88.05 dB	18,000	0.15
210 m	15	91.422 dB	15,000	0.564
245 m	15	95.41 dB	18,000	0.622
320 m	15	99.03 dB	25,000	0.88
395 m	15	102.56 dB	10,000	1.05

Table 12. Measurement Results for ORiNOCO ComboCard

From the captured files, it was also observed that packet errors started to be significant at signal Path Loss of about 91 dB. However the packet errors in this case were not as severe as the case for Linksys WPC54G.

In Figure 22 and Figure 23 we see the signal Path Loss and the PER respectively for the Orinoco wireless card.

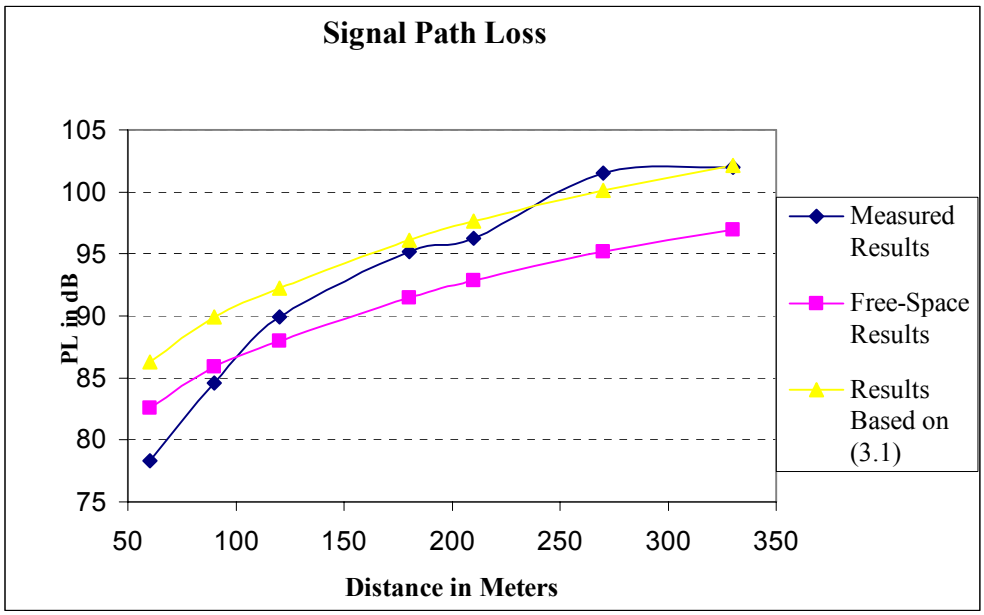

Figure 22. Orinoco Signal Path Loss Results

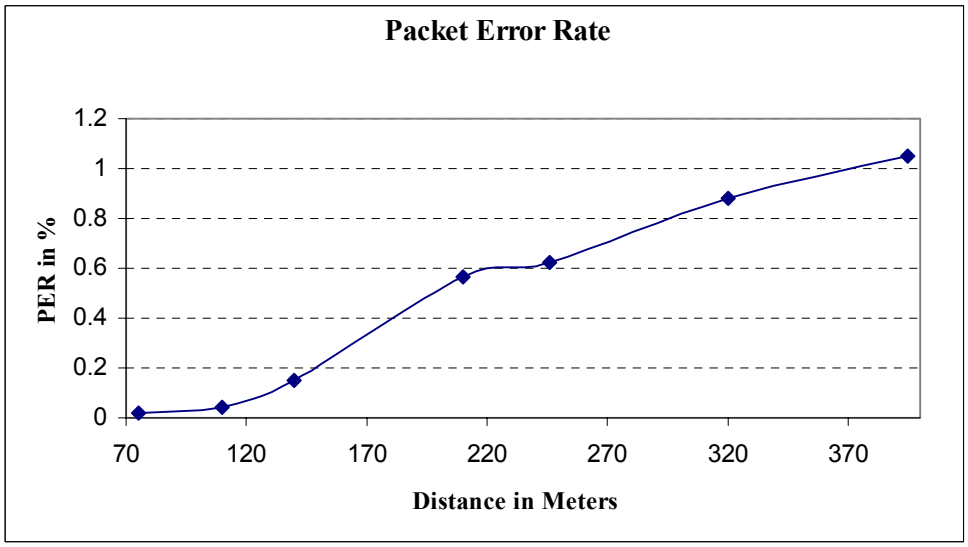

Figure 23. Measured Orinoco Beacon PER

As we see, the PER increases significantly after the 110 meters, and it also increases at the 245-meter point in this case.

The measurement results for the D-Link AirPlus XtremeG DWL-650 Wireless Adapter are tabulated in Table 13. Similar results due to the multipath effects at

the 110- and 245-meter point were observed. It is also interesting that the measured results were quite similar to the Equation (3.1) tabulated results. These results are illustrated in Figure 24.

Distance	Number of Captures	Average Signal Path Loss	Average Number of Captured Packets	Number of Error Packets (%)
75 m	15	79.88 dB	20,000	0.01
110 m	15	83.9 dB	25,000	0.05
140 m	15	89.88 dB	18,000	0.44
210 m	15	94.34 dB	15,000	1.08
245 m	15	96.3 dB	18,000	2.4
320 m	15	101 dB	25,000	4.24
395 m	15	102.6 dB	10,000	5.35

Table 13. Measurement Results for D-Link AirPlus XtremeG DWL-650

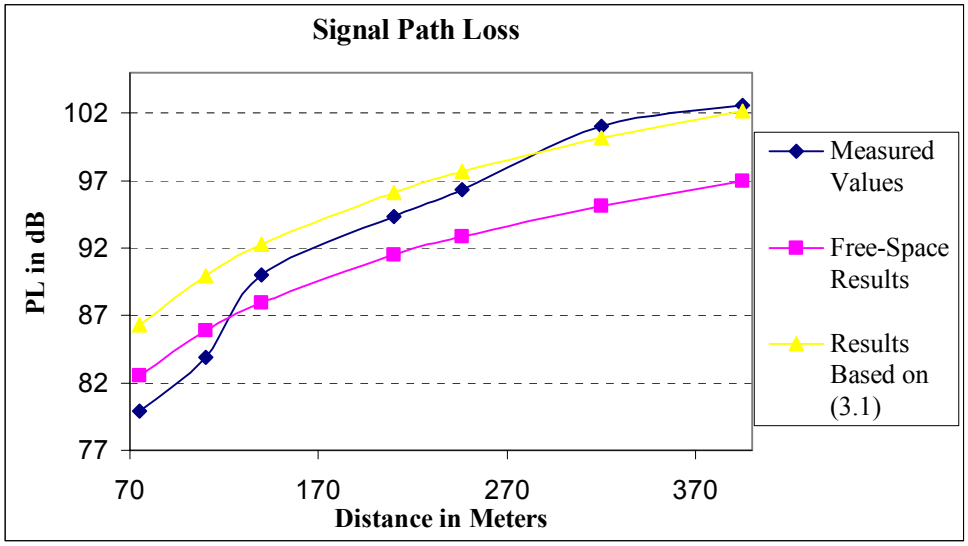

Figure 24. D-Link Signal Path Loss Results

From the captured files, it was also observed that packet errors started to be significant at the 210-meter point. This corresponds to a signal Path Loss of about 94 dB based on Table 13. The packet error also became more severe after the 320-meter point.

Based on the three sets of results, a combined table for performance comparison is presented in Table 14. Note here that, although we tried to detect the 802.11g wireless signal beyond the distance of 395 m, most of the times all three wireless cards could not establish a connection with the AP that we used.

Distance	Linksys		ORiNOCO		D-Link		Theoretical Equation (2.3) (dB)
	Path Loss (dB)	PER (%)	Path Loss (dB)	PER (%)	Path Loss (dB)	PER (%)	
75 m	79.25	0.193	78.34	0.021	79.88	0.01	82.545
110 m	85.2083	0.332	86.822	0.044	83.9	0.05	85.874
140 m	91.1665	1.91	88.05	0.15	89.88	0.44	87.969
210 m	93.8488	2.44	91.422	0.564	94.34	1.08	91.49
245 m	96.531	4.49	95.41	0.622	96.3	2.4	92.865
320 m	100.513	11.88	99.03	0.88	101	4.24	95.149
395 m	101.665	12.31	102.56	1.05	102.6	5.35	96.978

Table 14. Combined Measurement Results

From the combined results, it is quite obvious that the signal Path Loss was very similar for all three cases. But the PER was significantly lower when using the ORiNOCO ComboCard. Thus the ORiNOCO ComboCard performed better than both the D-Link and the Linksys WPC54G cards due to the lower PER, while the Linksys card had the highest error rate. This might be because the WPC54G card is developed only for home and office applications [13].

Figures 25 and 26 show the combined results for the signal Path Loss and the PER, respectively.

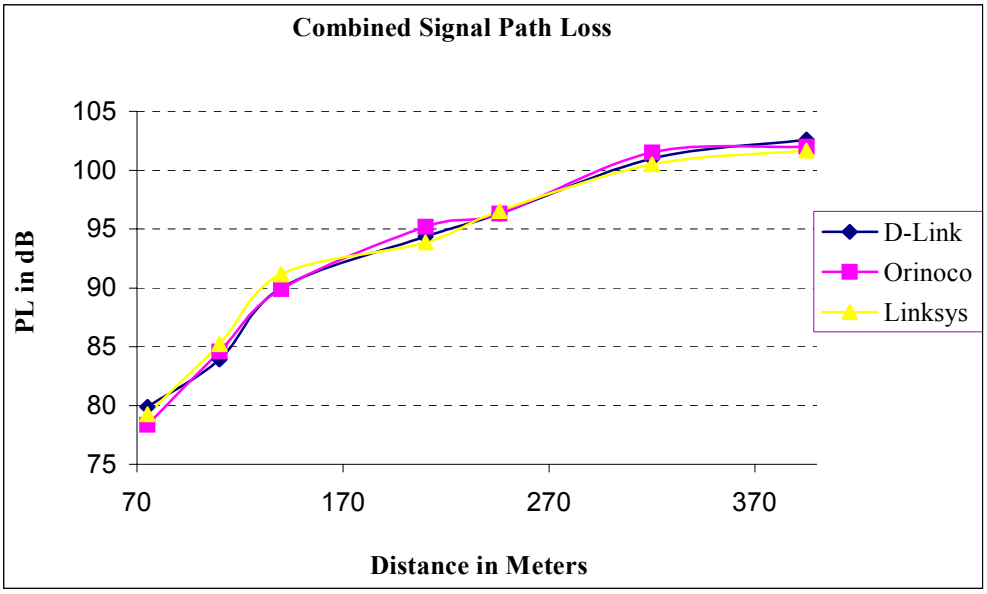

Figure 25. Combined Signal Path Loss Results

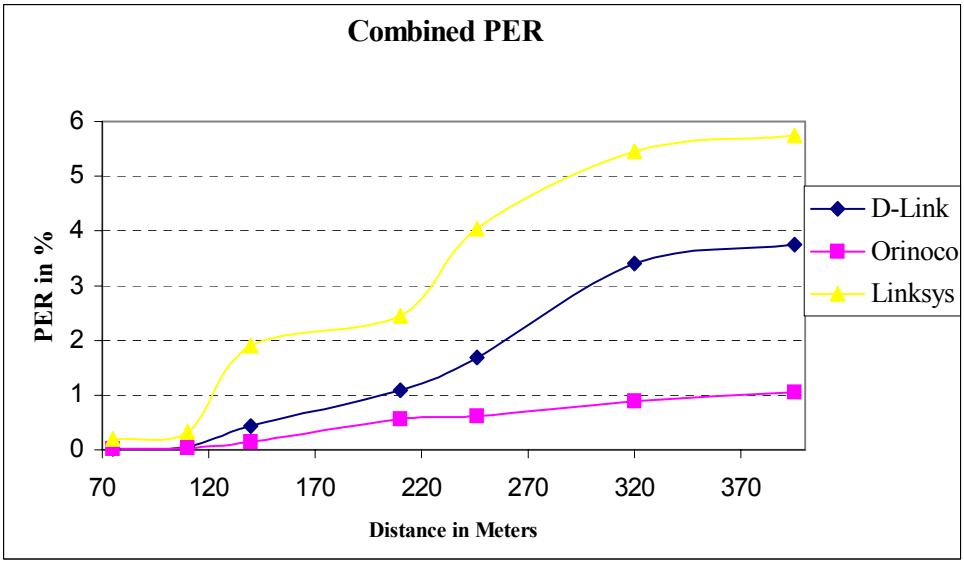

Figure 26. Combined PER Results

4. Sensitivity Measurements in LOS (Two-Ray Model)

It is obvious from the theoretical analysis of Chapter II that the heights of both the receiving and the transmitting antennas are crucial factors in the propagation path loss of microwave signals. Equation (2.6) shows that for higher heights of the transmitter and the

receiver antennas, h_t and h_r, respectively, the signal Path Loss is lower for a given distance. Since we are looking for a prototype system that may be used in military implementations, setting a transmitting AP at large heights may be desirable. Therefore we kept the receiver at the same height, but we positioned the transmitter on a higher position, still keeping the LOS clear. To further validate the results that suggested that the ORiNOCO ComboCard was the best of the three 802.11g cards, simple measurements for the LOS case were conducted.

a. Test Set-Up

The same set-up that was used for the previous measurement sensitivity was also used during this experiment. The AP was positioned at a height of 25 m on the beach of Monterey. Various measurements for distances at 500 m, 1000 m and at 1500 m were made. Therefore we created a signal Path Loss-PER profile regarding the specific situation. The measurement environment is shown in Figure 27.

Figure 27. LOS Measurement Environment (Two-Ray Model)

The location coordinates and distance with respect to the AP are tabulated in Table 15.

Location	Coordinates	Distance from Equation (2.9)
AP	$N36^{\circ}36'37.5"\ W121^{\circ}51'34.8"$	-
500 m	$N36^{\circ}36'30.5"\ W121^{\circ}51'52.7"$	494.78 m
1000 m	$N36^{\circ}36'23.1"\ W121^{\circ}52'10.71"$	997.5 m
1500 m	$N36^{\circ}36'15.88"\ W121^{\circ}52'28.7"$	1496.3 m

Table 15. Location Coordinates

b. Measurement Results and Analysis

The theoretical results based on the Two-Ray Model are tabulated below in Table 16. In Table 17, we present the summarized measured results for all three wireless cards tested. These results are detailed in Figures 28 and 29 below.

Location	Theoretical Two-Ray Model Signal Path Loss
500 m	73.01 dBm
1000 m	85.051 dBm
1500 m	92.095 dBm

Table 16. Two-Ray Model Signal Path Loss

Distance	Linksys		ORiNOCO		DWL	
	Path Loss (dB)	PER	Path Loss (dB)	PER	Path Loss (dB)	PER
500 m	77.2	0.18	75.6	0.094	78.9	0.105
1000 m	90	2.25	93.4	1.68	91.4	1.84
1500 m	101.75	8.74	102.6	4.31	99.7	5.89

Table 17. LOS Measurement Results (Two-Ray Model)

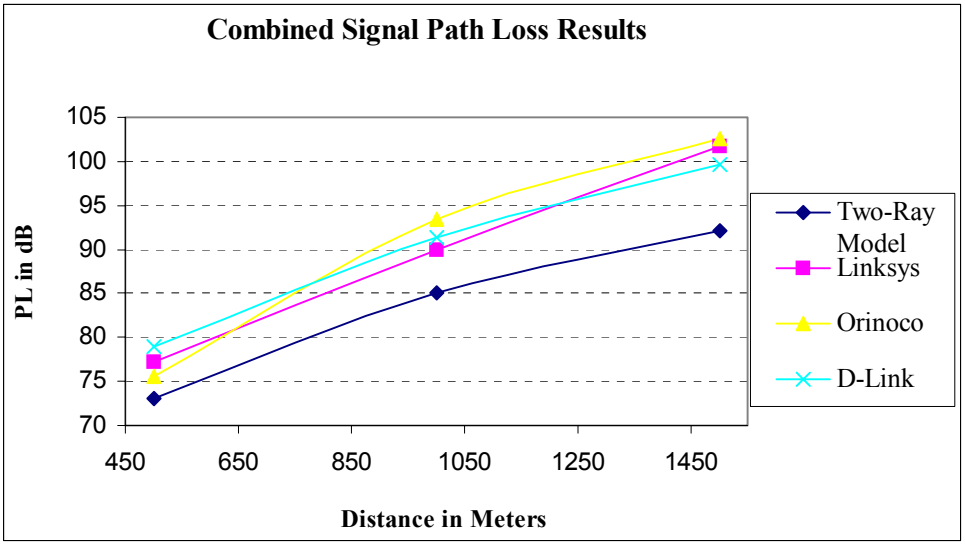

Figure 28. Two-Ray Model Signal Path Loss

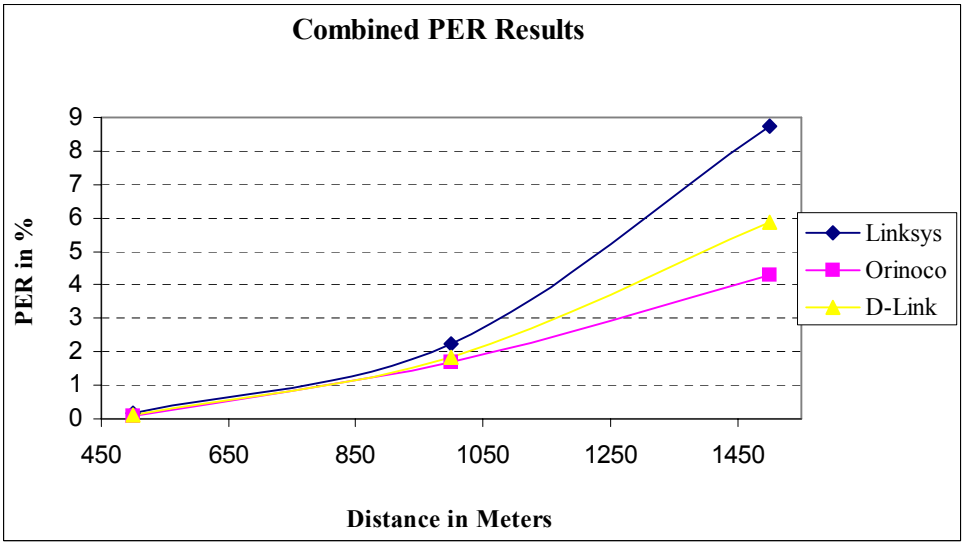

Figure 29. Two-Ray Model PER

The measurement results in Table 17 enhanced those obtained in the earlier measurement for LOS Free-Space situations. The ORiNOCO ComboCard performed best in both cases, providing the lowest PER. Note here that the results from all three cards deviated from the theoretical results of the two-ray model, most likely because of the multipath effect.

5. 802.11g Receiver Selection

Based on all the measurement data, the best 802.11g card for the prototype system was the ORiNOCO 11a/b/g ComboCard.

The Linksys WPC54G, ORiNOCO ComboCard and D-Link cost $100, $150 and $80, respectively. As we see the ORiNOCO ComboCard is not the cheapest one, but this increase in cost is insignificant when the better performance of the system is considered.

There is also an added advantage of using the ORiNOCO ComboCard for the prototype system. Because the ORiNOCO is an 11a/b/g compliant card, the resulting prototype system can detect signals from 802.11a and 802.11b compliant networks too.

D. FINAL CHOICE OF PROTOTYPE SYSTEM

Finally we can now answer the first question of the thesis. The commercially built prototype system that could detect and process wireless IEEE 802.11g wireless signals consists of the following components:

- Laptop Computer running on Windows XP Professional, with the configurations listed in Table 6. This Dell Latitude C840 laptop is not expected to cost more than $2,000.
- The Proxim Orinoco 11a/b/g ComboCard GOLD 8480-WD, which costs about $150.
- The AiroPeek NX protocol analyzer software, at a cost of $3,500 for a 12-month license and maintenance contract.

Lastly, adding all the above, the prototype system cost about $5,650.

E. SUMMARY

In this chapter we built a prototype system that is capable of detecting 802.11g WLANs and processing compliant wireless 802.11g signals. This development was based on the choices we made for the software and the hardware of the system.

The most proper software, the AiroPeek NX, was selected because of its previous efficient performance as a protocol analyzer, not because of its price.

The most important decision we had to make was the choice of the “receiver” of the system, i.e., the wireless card. This decision was based on the measurement results for three wireless cards, the Linksys, the Orinoco and the D-link card. As the experiment proved, all three cards had a similar performance regarding the signal path loss. But the

Orinoco card operated better regarding the PER of the received signals. Thus we used that card as the receiver of the system.

At this point we should note that the newly design system can detect and capture wireless signals up to distances of about 400 m from the wireless source, providing there is a clear LOS between the source and the system. Beyond this distance the system can hardly even sense the existence of a WLAN. Of course this distance metric may be decreased significantly if the surrounding environment introduces heavy multipath effects or when there is no LOS connection between the source and the receiver.

The next chapter is crucial because it refers to the evaluation performance of the prototype system and also proves that this system can provide good results during military operations.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PERFORMANCE TEST AND RESULTS

The first objective of this work was addressed in the third chapter. Thus we built a prototype system that was a useful tool for detecting and analyzing wireless 802.11g signals. So the point of interest of this chapter is to answer the second question of the thesis – What is the detection performance of the prototype hardware and software solution for all three choices of security that can be implemented (that is, (1) no WEP, (2) 64-bit WEP, and (3) 128-bit WEP)?

A. PERFORMANCE TEST SETUP

The test setup for the measurement performance of our prototype system is shown in Figure 30.

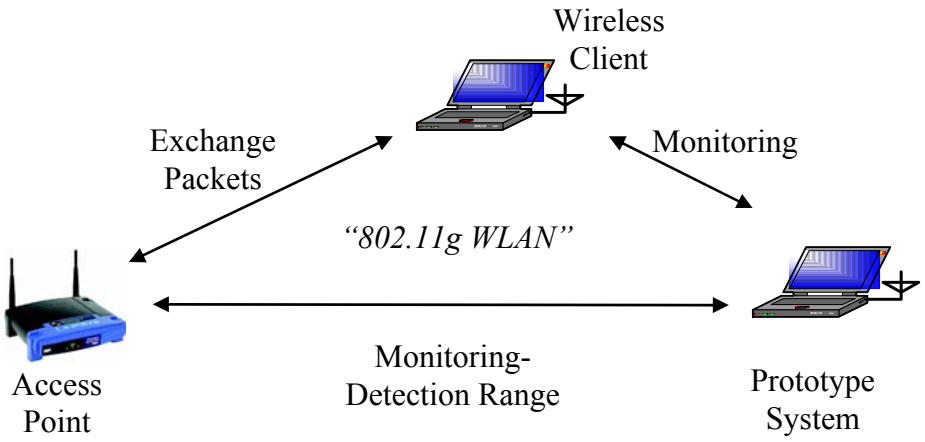

Figure 30. Performance Set Up

The test system consisted of the following three components:

- The first component was a wireless AP that was a "stand-alone" device. It was not connected to any wired network, but it only responded to the wireless ping request packets that were transmitted by a wireless client.
- The second component was the wireless client that triggered the AP transmitting ping request messages. In this chapter, the AP and the wireless client formed a "system."

- The third component was the newly designed prototype system with the WildPacket software installed to the laptop. The prototype system monitored the "wireless network" and measured the data link rates of the 802.11g signals and the PER. These measurements helped us evaluate the performance of the newly designed prototype system.

As noted above we monitored the established wireless connection between the AP and the wireless client, measuring the data rates and the errors of the network, as we moved the prototype system away from that established connection. The AP and the wireless client were positioned at a distance of 70 cm from each other, ensuring high data transmission rates. Using the platform described in the previous chapter, the AP was set at a height of 305 cm. In this test, three different sets of available equipment were used, namely the Linksys system, the ORiNOCO system and the D-Link system. Both the ORiNOCO and the D-Link system are commonly used for commercial/industrial WLAN networks, while the Linksys system is mainly used for home-based WLAN. All three systems were tested under the three security options used by the 802.11g.

The measurement environment for LOS was the same as that used in Chapter III. The performance of the prototype system under the LOS environment was evaluated using the ping packet with a length of 32 bytes. For the measurements, the prototype system was placed at distances of 75 m, 110 m, 140 m, 245 m, 320 m and 395 m from the AP to capture the transmitted PING packets, exactly at the same locations as those of the previous chapter.

B. RESULTS AND ANALYSIS

1. Linksys System

The Linksys WAP54G AP was paired up with the WPC54G Card in the wireless client so that no incompatibility issues existed between the AP and the wireless client adaptor. As already mentioned, the transmitted power of the WAP54G was 15 dBm.

The LOS measurement results for the PING packets are shown in Table 18. Note that the Average Data Link Rate decreased when the separation distance between the AP and the wireless signal receiver increased.

Separation Distance	No of Captures	Average Data Rate (Mbps)			Average PER (%)		
		No WEP	64-bit WEP	128-bit WEP	No WEP	64-bit WEP	128-bit WEP
75 m	8	35.67	32.2774	31.7634	0.08	0.16	0.67
110 m	8	31.24	28.7309	29.5684	0.15	0.52	1.15
140 m	9	29.6	24.1	27.1713	1.52	0.83	4.63
210 m	6	20.4	22.9	22.82	2.3	1.92	5.95
245 m	8	12.1	8.626	9.78628	4	3.2	7.6
320 m	8	3.4	1.5	1.01	4.17	5.6	9.6
395 m	8	2.1	0.69	0.7	8.4	7.22	10.34

Table 18. Measured LOS Linksys System Results

These results show that the Average Data Link Rate was related to the link condition between the AP and the receiver. It is also interesting that the average data transmission rate was almost the same for all three security options (no-WEP, 64-bit WEP and 128-bit WEP). The results also showed that, in all three conditions, the number of packets received in error increased when the separation distance was increased.

The average PER for the various distances is also shown in Figure 31.

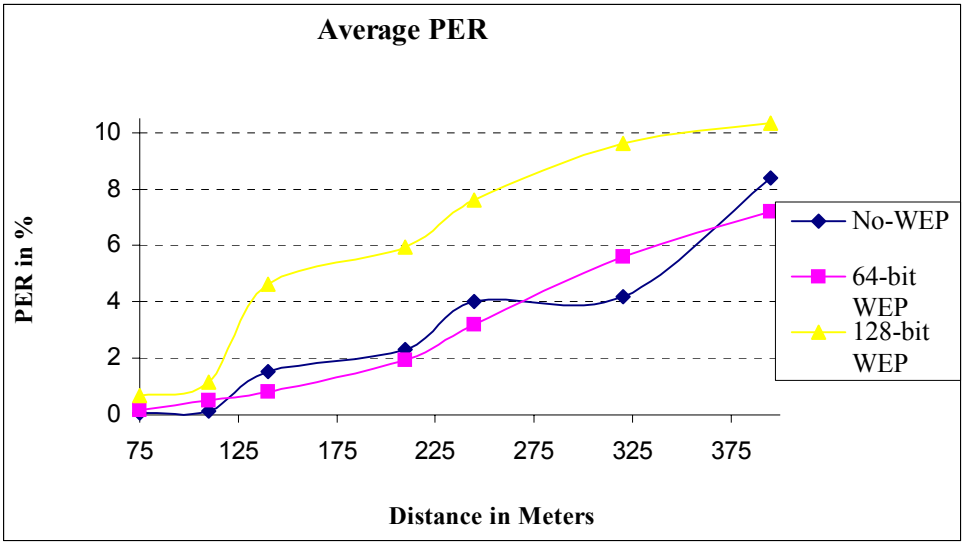

Figure 31. Average Measured PER for the Linksys System

It is interesting to note that the average PER was similar for the no-WEP and 64-bit WEP cases for the various distances, but it increased to about 15% in the 128-bit case. We can also see an increase of the Average PER after the 110- and the 210-meter points. This is a conclusion that agrees with the sensitivity measurement results of the previous chapter.

2. ORiNOCO System

The ORiNOCO system consisted of the AP2000 AP installed with the 802.11g upgrade kit, operating with ORiNOCO ComboCard GOLD in the wireless client. The Orinoco AP2000 is shown in Figure 32.

Figure 32. Orinoco AP 2000 (From Ref. 18.)

This AP provides a high-speed of 54 Mbps and supports 802.11b, 802.11g and 802.11a standards, all in one platform. [18]

Based on the AP2000 user guide [18], the maximum transmitted power is $+17$ dBm and the receiving sensitivity varies from -85 dBm at 6 Mbps to -65 dBm at 54 Mbps. The antenna for the 802.11g radio has a gain of 5 dBi. The theoretical outdoor transmission distances claimed by Orinoco are 40 m with a data rate of 54 Mbps and 400 m for 6 Mbps [18]. These data rates are theoretical, without taking into consideration the ACK time needed for a successful transmission or the time needed for the extra overhead bits of a data packet.

The LOS measurement results for PING packets are shown in Table 19.

Separation Distance	**No of Captures**	**Average Data Rate (Mbps)**			**Average PER (%)**		
		No WEP	**64-bit WEP**	**128-bit WEP**	**No WEP**	**64-bit WEP**	**128-bit WEP**
75 m	6	38.24	34.18	33.9	0.063	0.19	0.74
110 m	6	34.18	31.22	32.1	0.16	0.38	1.44
140 m	6	29.33	27.65	24.3	1.09	1.08	2.87
210 m	6	28.5	25.2	22.3	2.42	2.24	4.28
245 m	6	11.9	18.3	12.9	3.1	4.06	6.03
320 m	6	4.4	2.8	1.8	5.69	6.44	8.95
395 m	6	2.2	2.55	2.31	6.88	7.31	9.6

Table 19. Measured LOS Orinoco System Results

Due to the much higher effective transmit power of the AP2000, the results showed that the packets captured were generally at higher data rates compared to the

Linksys system. The comparison of the data in Table 18 and Table 19 enhanced the earlier suggestion that the PER performance of the prototype system decreases with an increased data rate.

In Figure 33 below the average PER results for the Orinoco system are presented. The similarity of the errors between the two lower security situations (no-WEP and 64-bit WEP) is still obvious, and the increase of the PER in the 128-bit WEP situation was about 10% compared to the previous two functions. It is still true that the 110- and 210-meter points are distances at which the average PER suddenly increases.

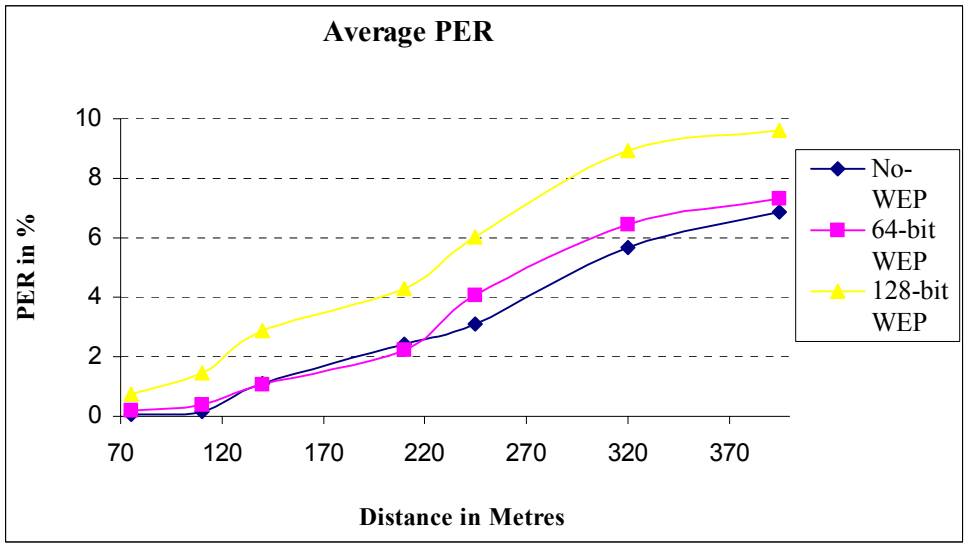

Figure 33. Measured Average PER for the Orinoco System

3. D-Link System

The D-Link system consisted of the Cisco AP1200 AP installed with the 802.11g upgrade kit, operating with the D-Link AirPlus XtremeG DWL-650 Wireless Adapter in the wireless client. The AP1200 is shown in Figure 34. In this case we combined an AP and a wireless card from different vendors since a D-Link AP was not available at NPS.

Figure 34. Cisco AP 1200 with 802.11g Radio Kit (From Ref. 19.)

Based on the datasheet [19], the AP1200 has a maximum output power of $+16\,\text{dBm}$. The receiving sensitivity ranges from $-94\,\text{dBm}$ at 1 Mbps to $-72\,\text{dBm}$ at 54 Mbps. When the patch antenna is used, it provides a gain of $+2\,\text{dBi}$. This offers the AP1200 an effective transmitted power of $+18\,\text{dBm}$. The theoretical outdoor distances are $76\,\text{m}$ at 54 Mbps and $396\,\text{m}$ at 6 Mbps. Again Cisco has not calculated the ACK time needed for a successful transmission or the time needed for the extra overhead bits of a data packet. [19]

The LOS measurement results for PING packets are shown in Table 20. The data rate for PING packets were lower than 39 Mbps. Again, the results suggested that the PER increases with an increase in the data rate of the captured packets. The same phenomenon of transmitting data packets at lower data rates, as the separation distance increases, was also observed.

Separation Distance	No of Captures	Average Data Rate (Mbps)			Average PER (%)		
		No WEP	64-bit WEP	128-bit WEP	No WEP	64-bit WEP	128-bit WEP
75 m	6	39.2	39.88	35.6	0.13	0.33	1.1
110 m	6	36.26	27.44	30.3	0.22	0.25	1.68
140 m	6	30.65	26.4	24.8	1.2	1.12	3.6
210 m	6	24.236	21.5	23.2	2.15	1.99	5.4
245 m	6	20.7	16.7	18	4.5	3.43	6.58
320 m	6	3.6	1.9	2.31	4.15	6.88	10.44
395 m	6	2.43	2.9	2.05	8.55	9.13	11.56

Table 20. Measured LOS D-Link System Results

The average PER results of the D-Link system for the various distances are illustrated in Figure 35. Note that the previous conclusions were still in effect for this system as well. That is, both the no-WEP and the 64-bit WEP implementations had almost the same average PER for the various distances, and they had a superior average PER from the 128-bit implementation of about 10%. We also see that, at the 110- and 210-meter points, the average PER had a relatively sudden increase.

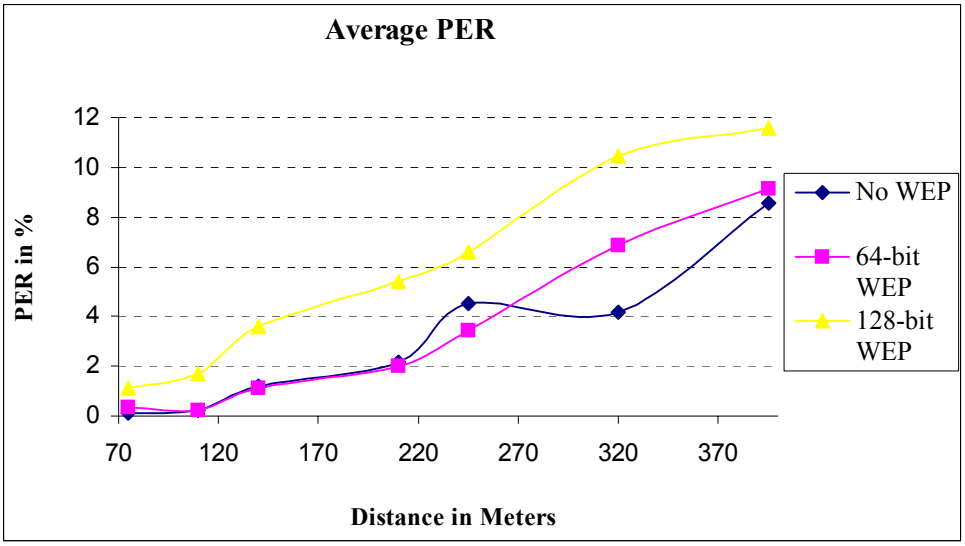

Figure 35. Measured Average PER for the D-Link System

Finally an important conclusion in comparing the results of all three systems is that the Average PER performance of the prototype system depends on the data rate of the packets being captured – the number of packets captured in error increases with an increased data rate of the packets.

C. PROTOTYPE PERFORMANCE SUMMARY

All the measurement results suggested that the performance of the prototype system depends very much on the characteristics of the 802.11g signal to be captured. The data collected for PING packets can be summarized in Table 21. The data points indicated that higher PER appears at longer distances and with higher data rates.

Distance	System	Average Data Rate (Mbps)			PER (%)		
		No-WEP	64-bit WEP	128-bit WEP	No-WEP	64-bit WEP	128-bit WEP
75 m	Linksys	35.67	32.2774	31.7634	0.08	0.16	0.67
	Orinoco	38.24	34.18	33.9	0.063	0.19	0.74
	D-Link	39.2	39.88	35.6	0.13	0.33	1.1
110 m	Linksys	31.24	28.7309	29.5684	0.15	0.52	1.15
	Orinoco	34.18	31.22	32.1	0.16	0.38	1.44
	D-Link	36.26	27.44	30.3	0.22	0.25	1.68
140 m	Linksys	29.6	24.1	27.1713	1.52	0.83	4.63
	Orinoco	29.33	27.65	24.3	1.09	1.08	2.87
	D-Link	30.65	26.4	24.8	1.2	1.12	3.6
210 m	Linksys	20.4	22.9	22.82	2.3	1.92	5.95
	Orinoco	28.5	25.2	22.3	2.42	2.24	4.28
	D-Link	24.236	21.5	23.2	2.15	1.99	5.4
245 m	Linksys	12.1	8.626	9.78628	4	3.2	7.6
	Orinoco	11.9	18.3	12.9	3.1	4.06	6.03
	D-Link	20.7	16.7	18	4.5	3.43	6.58
320 m	Linksys	3.4	1.5	1.01	4.17	5.6	9.6
	Orinoco	4.4	2.8	1.8	5.69	6.44	8.95
	D-Link	3.6	1.9	2.31	4.15	6.88	10.44
395 m	Linksys	2.1	0.69	0.7	8.4	7.22	10.34
	Orinoco	2.2	2.55	2.31	6.88	7.31	9.6
	D-Link	2.43	2.9	2.05	8.55	9.13	11.56

Table 21. Summarized Measured Results for PER of All Three Systems

A more useful presentation of the data from Table 21 is shown in the following figures for all three security implementations. Although there were only three systems tested and the capture trials were no more than ten per distance for each case, the graphs provide some means to estimate the performance of the prototype system when it is used to capture small data packets.

Figure 36 to Figure 44 present the expected PER of the prototype system for all three security options at various distances. All these graphs were created with the help of

the Microsoft Excel. For the completion of them, the data points from the Table 21 of all three systems were input into Excel. Then, we used the ability of Excel to create a linear trend line/graph using at least two data points.

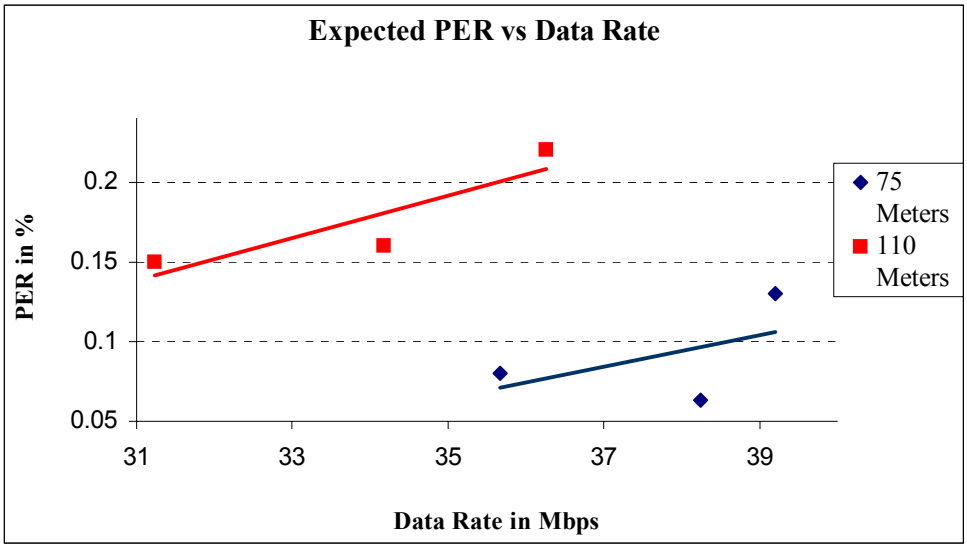

Figure 36. Expected PER in No-WEP Situation

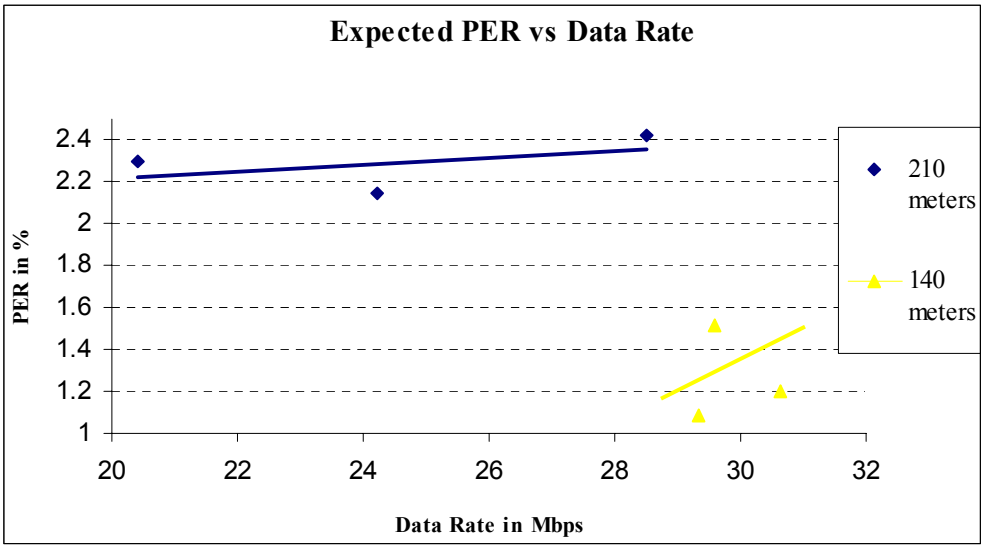

Figure 37. Expected PER in No-WEP Situation

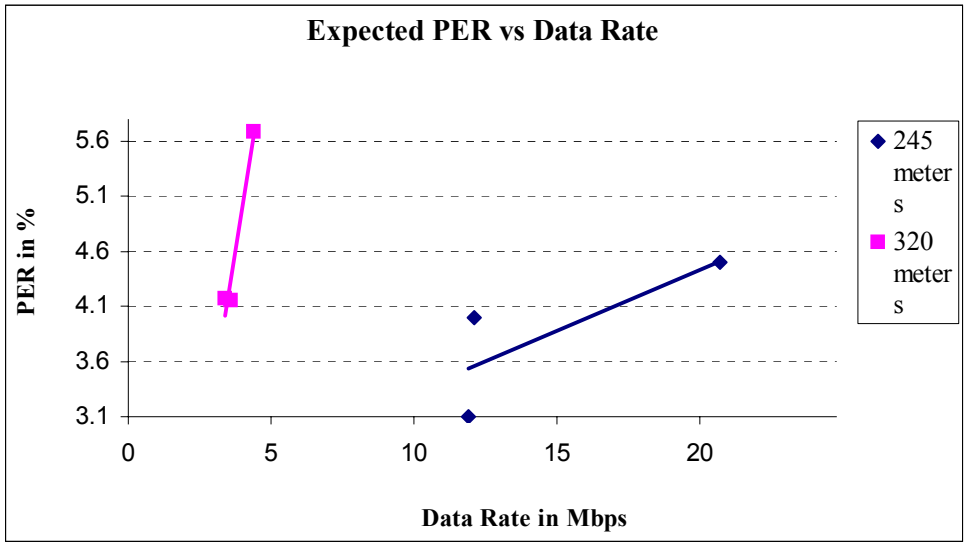

Figure 38. Expected PER in No-WEP Situation

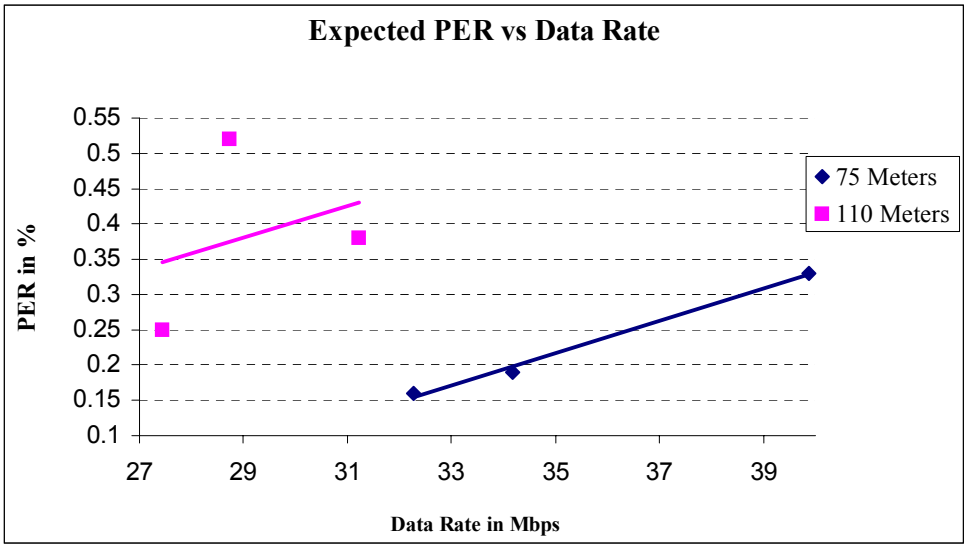

Figure 39. Expected PER in 64-bit WEP Situation

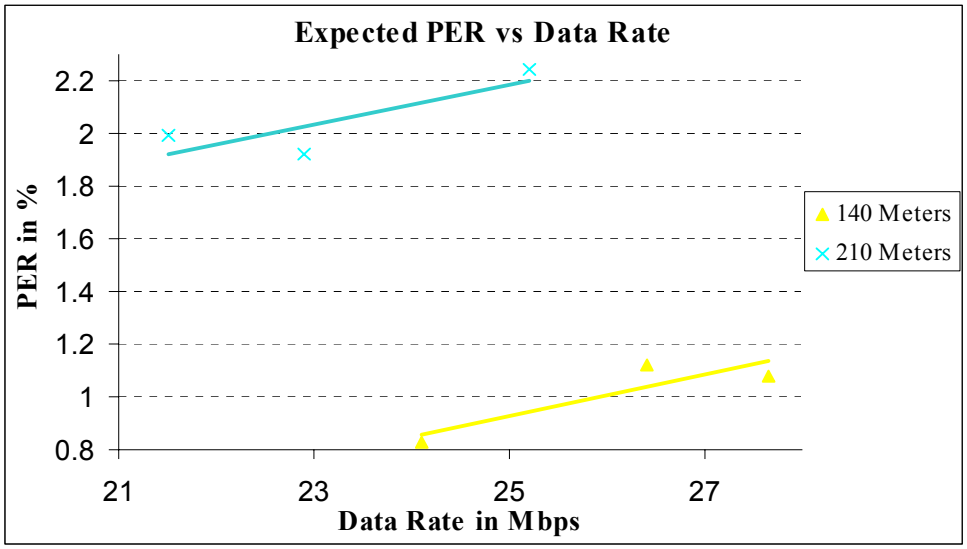

Figure 40. Expected PER in 64-bit WEP Situation

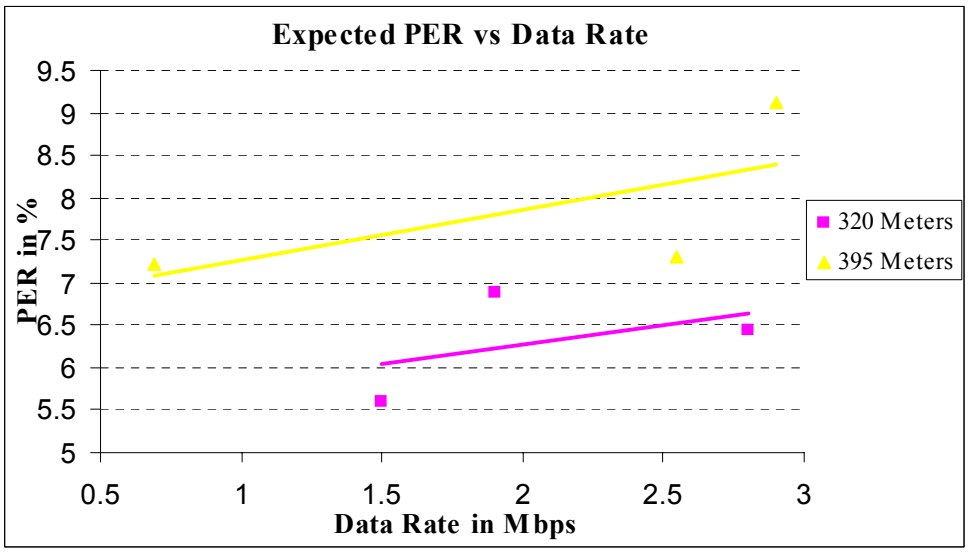

Figure 41. Expected PER in 64-bit WEP Situation

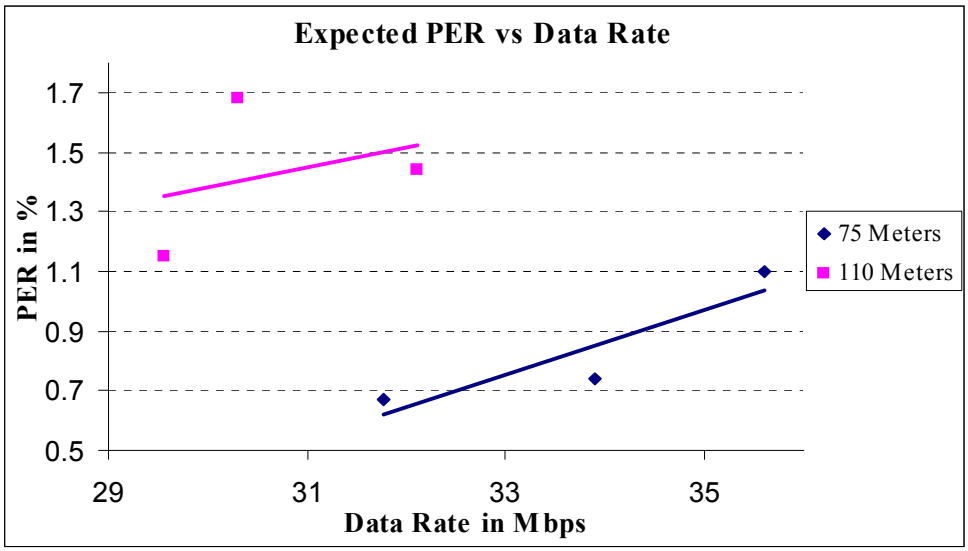

Figure 42. Expected PER in 128-bit WEP Situation

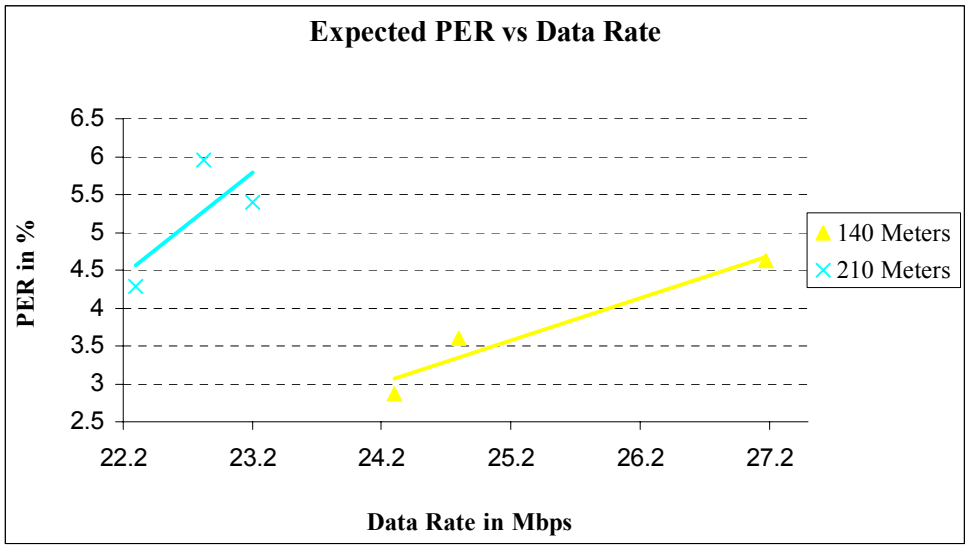

Figure 43. Expected PER in 128-bit WEP Situation

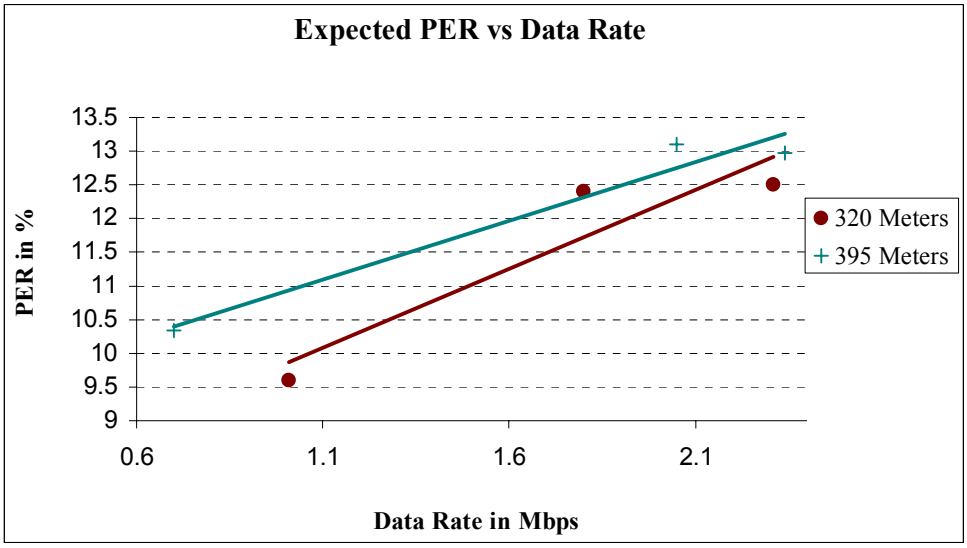

Figure 44. Expected PER in 128-bit WEP Situation

As a conclusion of the performance test of our prototype system we infer that, when the system operates without using the WEP mechanism, the results are similar to the results when the system operates using 64-bit WEP. They both offer effective performance with a very low PER of about 10% maximum, even at 395 m away from the AP. Of course at that distance the average data rate decreases to about 1 Mbps. Moreover, if we still want to maintain a high transmission data rate, we accomplish that by using the system up to 210 m away from the AP, having fairly low PER (about 2%). At such distances, the average data rate is never less than 20 Mbps, which is significantly high.

Unfortunately, during the third case, when the prototype system operates using 128-bit WEP, we notice that the performance of the system slightly decreases. The 395-meter point remains the distance limit and the average data rate is also about 0.5 Mbps to 1 Mbps. But the PER is greater and it ranges from 10% to 13%. If we want to maintain high data rates of about 20 Mbps, we must position the prototype system up to 210 m away from the source, but suffer a higher PER, about 4% to 6%. This value is about three times greater than the PER of the two previous cases.

Finally we should point out that even when the PER is about 10% to13%, the prototype system remains reliable, and it could be used in military operations.

In the next chapter, by using the newly developed prototype system, we determine the average transmission rate and the actual throughput data rate of the 802.11g WLAN. This experiment helps us prove that the IEEE 802.11g standard is a very powerful and useful tool for military operations, especially due to the high data rate it offers.

V. 802.11G LINK PERFORMANCE

We proved in the previous chapter that the prototype system performs well, with a PER no more than 13%, in situations where the LOS between the AP and the wireless client is preserved and given that the receiver will not be at distances greater than 400 m from the AP. In this chapter, taking advantage of those results, we address the final question of this thesis using this prototype system. Three 802.11g systems operated outdoors, and the prototype system was used to determine the data link rate and the actual throughput achieved by the 802.11g WLAN network at various ranges. This was done for all three security implementations that are offered by the 802.11g standard. These implementations are the use of no-WEP, of a 64-bit WEP and of a 128-bit WEP. Finally the actual measured performance is compared with the advertised ranges.

A. PERFORMANCE TEST SETUP

The test setup for measuring the data link rate is shown in Figure 45 below. In this test, the same three sets of available equipment from Linksys, ORiNOCO, and D-Link were used.

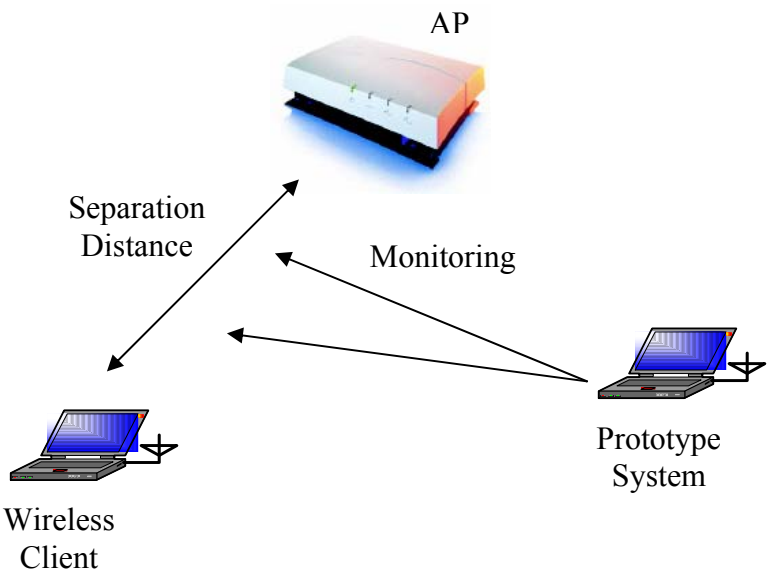

Figure 45. Link Performance Test Setup

The LOS measurement environment in this test was presented in Figure 19. The locations of the AP and the measurement position where the wireless client was placed were exactly the same as those listed in Table 8. We should note here that, although this process is similar to the one in the previous chapter, there are some important differences. In this case the AP and the prototype system remained in the same position throughout the whole experiment and the wireless client was positioned to various distances away from the AP. The prototype system was stationed in the vicinity of the LOS of the AP and of the wireless client to capture the 802.11g packets (ping requests and ping replies) that are transferred between them. Thus, the system monitored the simple 802.11g WLAN network and measured the transmission rates, the PER and the retry packets of the established 802.11g connection.

B. RESULTS AND ANALYSES

1. Linksys System

The measurement results for the Linksys system are shown in Table 22. To compute the average data rate, we computed both the "ping packet" transmission rate and the "acknowledge (ACK) packet" transmission rate. The "ACK packet" transmission rate is generally lower than the corresponding data packet rate, and we should note that it is not always the lowest available rate of the 802.11g (1 Mbps).

Separation Distance	Average Data Rate (Mbps)			Retry Packets (%)		
	No-WEP	64-bit WEP	128-bit WEP	No-WEP	64-bit WEP	128-bit WEP
75 m	36.2	33.42	32.92	4.8	3.56	4.1
110 m	32.81	28.7	28.9	8.22	5.43	7.15
140 m	31.4	25.3	26.8	9.17	8	8.4
210 m	22	24.5	23.5	12.32	10.95	10.21
245 m	12.4	9.5	7.8	14.95	13.38	13.1
320 m	5.7	2.8	4	16.0123	14.65	15.11
400 m	2.21	0.84	0.68	16.23	14.68	15.33

Table 22. Measured Linksys System Results

The number of the percentage of retry packets refers to the whole number of packets that were captured. These retry packets were retransmitted from the AP or from the wireless client by request of the receiver end.

As expected, the average data link rate was much lower than the advertised 54 Mbps, and it gradually decreased as the distance between the AP and the wireless client increased. Also, in general, the number of retry packets increased as the separation distance increased.

In Figure 46, the Linksys system Average Data Rate for distances up to 400 m is presented for the three different security implementations. It is obvious that the transmission rate decreased at about 5 Mbps average as the security option increased from use on no-WEP up to the use of the 128-bit WEP, which is not so significant.

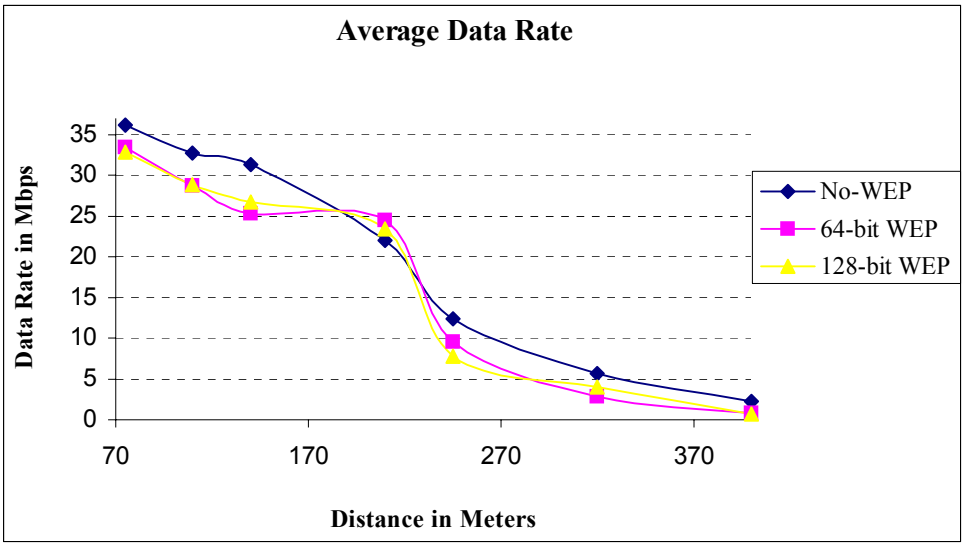

Figure 46. Measured Linksys System Average Data Rate

2. ORiNOCO System

The results for ORiNOCO system are presented in Table 23. Likewise, the data rate changed and shifted downward as the separation distance increased, and the retry packets increased when the separation distance increased.

Separation Distance	Average Data Rate (Mbps)			Retry Packets (%)		
	No-WEP	64-bit WEP	128-bit WEP	No-WEP	64-bit WEP	128-bit WEP
75 m	38.45	34.8	33.1	5.2	4.87	4.4
110 m	35.6	31.9	33.6	7.34	6.2	7.51
140 m	30.4	28.8	26.8	9.81	7.89	8.33
210 m	26.2	22.5	24.3	13.7	11.3	14.2
245 m	12.3	16.77	10.3	14.66	14.99	15.6
320 m	3.6	2.97	1.56	17.54	18.5	18.7
400 m	1.74	2.01	1.64	17.88	18.99	19.1

Table 23. Measured Orinoco System Results

Figure 47 shows the achieved Data Link Rate at various distances in the ORiNOCO system.

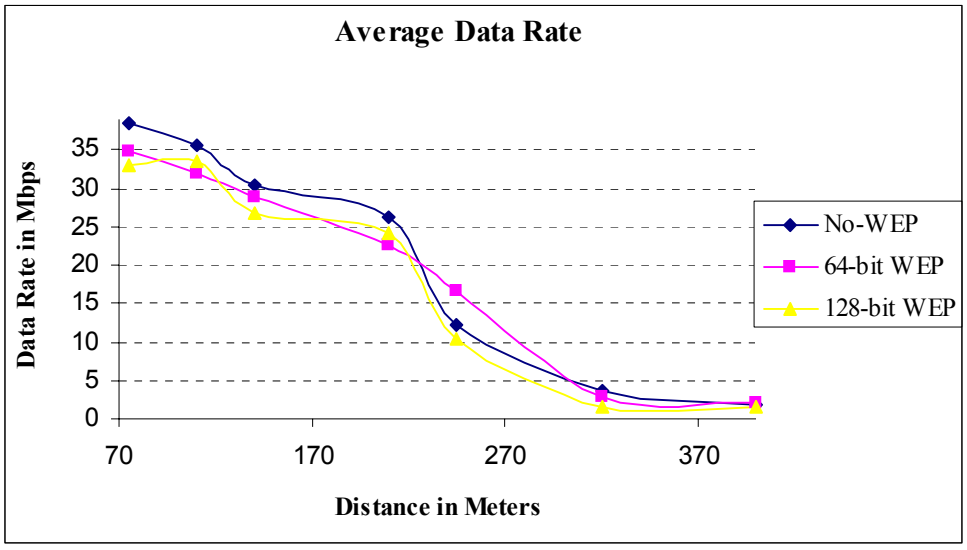

Figure 47. Measured Orinoco System Average Data Rate

It is interesting to note the sudden decline in the transmission rate after the 210-meter point, which also appeared in the Linksys system. This sudden decrease occurred because of the multipath effect and was due to the increased transmission path loss.

3. D-Link System

The measurement results for the D-Link system are listed in Table 24 below.

Separation Distance	Average Data Rate (Mbps)			Retry Packets (%)		
	No-WEP	64-bit WEP	128-bit WEP	No-WEP	64-bit WEP	128-bit WEP
75 m	40.2	40.74	36.7	3.1	4.1	5.2
110 m	37.45	28.98	31.7	7.8	6.3	7.4
140 m	31.86	27	24.31	10.1	8.2	9.8
210 m	25.8	22.67	23.64	13.8	11.4	12.9
245 m	20.5	14.56	11.5	14.3	13.5	14.5
320 m	3.22	1.95	2.21	16.65	17.1	17.1
400 m	2.55	2.66	1.97	16.8	17.8	16.34

Table 24. Measured D-Link System Results

As with the previous two cases, the data link rate of the 802.11g traffic decreased as the separation distance increased. These results are shown in Figure 48 below.

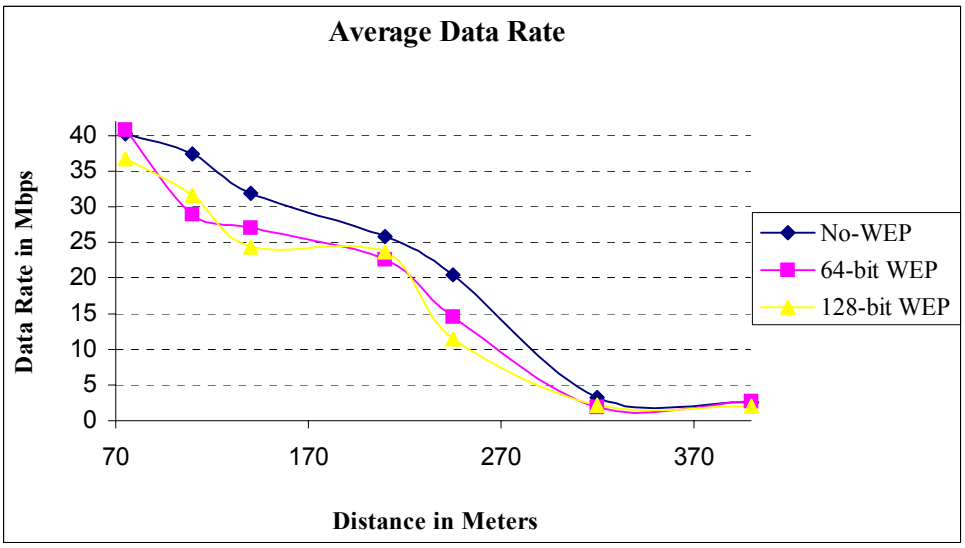

Figure 48. Measured D-Link System Average Data Rate

In the D-Link system, the no-WEP implementation seemed to be more efficient than the other two cases (use of 64-bit and 128-bit WEP), while the sudden decrease after the 210-meter point was still present because of the multipath effect.

C. SUMMARY OF 802.11G LINK PERFORMANCE

The average data link rate of the three 802.11g systems is summarized in Table 25. The decrease of the average data link rate as the separation distance increased can be clearly observed in all cases.

Separation Distance	Average Data Link Rate (Mbps)								
	Linksys			ORiNOCO			D-Link		
	No-WEP	64-bit WEP	128-bit WEP	No-WEP	64-bit WEP	128-bit WEP	No-WEP	64-bit WEP	128-bit WEP
75 m	35.67	32.27	31.76	38.24	34.18	33.90	39.20	39.88	35.60
110 m	31.24	28.73	29.56	34.18	31.22	32.10	36.26	27.44	30.30
140 m	29.60	24.10	27.17	29.33	27.65	24.30	30.65	26.40	24.80
210 m	20.40	22.90	22.82	28.50	25.20	22.30	24.23	21.50	23.20
245 m	12.10	8.62	9.78	11.9	18.30	12.90	20.70	16.70	18.00
320 m	3.40	1.50	1.01	4.40	2.80	1.80	3.60	1.90	2.31
400 m	2.10	0.69	0.70	2.20	2.55	2.31	2.43	2.90	2.05

Table 25. Combined Measured Results

These data are also graphically presented for the no-WEP situation in Figure 49. We observe that the 802.11g network can offer an effective range of more than 400 m, but the average packet transmission rate is very low, about 1.5 Mbps or less.

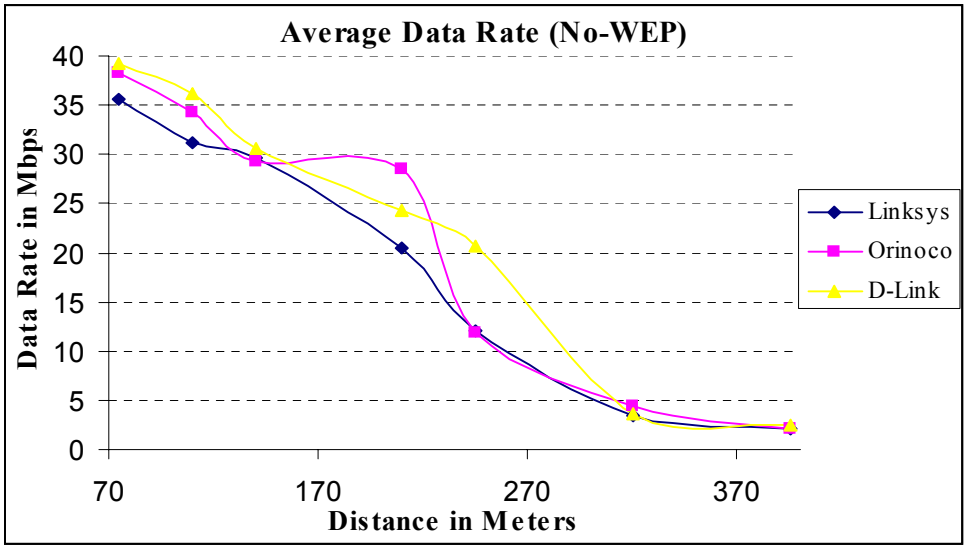

Figure 49. Measured Outdoor Data Link Rates of 802.11g

D. ACTUAL MEASURED THROUGHPUT OF 802.11G

As Figure 49 illustrates, the Outdoor Link Transmission Rate was lower than the advertised 54 Mbps, even at small distances from the AP. Besides the fact that the theoretical approach is always more optimistic than the real situation, there are two basic reasons for this difference:

- The first reason is that the maximum data rate of 54 Mbps is referred to a LOS propagation path. When we examine the outdoor transmission rate, we must always deal with multipath effects that cannot be computed in advance.
- The second reason is that, in a WLAN, a packet is considered as successfully transmitted only when the corresponding ACK packet is received. Otherwise this packet is retransmitted and the wireless traffic becomes heavier. In our study, we also computed the time needed for the ACK packet. Thus the overall "packet transmission" rate is not as high as the advertised 54 Mbps. [1]

Moreover, when a user is connected to a WLAN, he or she will never be able to transmit or to receive pure data with the maximum 54 Mbps or even with the maximum measured transmission rate of about 40 Mbps (Table 25). From a user's point of view, there is a reason for this reduction in the data transmission rate. The maximum 54 Mbps is for transmitted bits generally, whether these bits are information/data bits or whether

they are header or any other kind of overhead bits. This means that the 54-Mbps rate is referred to the theoretical bit transmission rate, and it is also completely different from the actual throughput rate that considers the overhead bits.

In Figures 50 and 51, we present an example of one of the wireless data packets that was captured and decoded by the AiroPeek NX, during the performance evaluation of the 802.11g. That specific packet was transmitted without the use of WEP. The AiroPeek NX can "decode" any packet and explain the use of the bits that form that specific packet. [12]

```
Packet Info
  Flags:                0x00
  Status:               0x00
  Packet Length:        96
  Timestamp:            10:29:34.783562000 02/06/2004
  Data Rate:            48  24.0 Mbps
  Channel:              6
  Signal Level:         22%
  Signal dBm:           -79

802.11 MAC Header
  Version:              0  [0 Mask 0x03]
  Type:                 %10  Data  [0]
  Subtype:              %0000  Data Only  [0]
Frame Control Flags:    %00000010  [1]
                        0... .... Non-strict order
                        .0.. .... WEP Not Enabled
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..1. Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Destination:          00:06:25:42:C2:23  Linksys Group:42:C2:23  [4-9]
  BSSID:                00:06:25:3C:D0:EB  Linksys Group:3C:D0:EB  [10-15]
  Source:               00:06:25:3C:D0:EB  Linksys Group:3C:D0:EB  [16-21]
  Seq. Number:          2119  [22-23 Mask 0xFFF0]
  Frag. Number:         0  [22 Mask 0x0F]
802.2 Logical Link Control (LLC) Header
  Dest. SAP:            0xAA  SNAP  [24]
  Source SAP:           0xAA  SNAP  [25]
  Command:              0x03  Unnumbered Information  [26]
  Vendor ID:            0x000000  [27-29]
  Protocol Type:        0x0800  IP  [30-31]
```

Figure 50. Decoded Data Packet

```
IP Header - Internet Protocol Datagram
  Version:                4  [32 Mask 0xF0]
  Header Length:          5  (20 bytes)  [32 Mask 0x0F]
  Type of Service:        %00000000  [33]
                          000. .... Precedence: Routine
                          ...0 .... Normal Delay
                          .... 0... Normal Throughput
                          .... .0.. Normal Reliability
                          .... ..0. ECT bit - transport protocol will ignore the
    CE bit
                          .... ...0 CE bit - no congestion
  Total Length:           60  [34-35]
  Identifier:             9030  [36-37]
Fragmentation Flags:      %000  [38 Mask 0xE0]
                          0.. Reserved
                          .0. May Fragment
                          ..0 Last Fragment
  Fragment Offset:        0  (0 bytes)  [38-39 Mask 0x1FFF]
  Time To Live:           255  [40]
  Protocol:               1  ICMP - Internet Control Message Protocol  [41]
  Header Checksum:        0x1433  [42-43]
  Source IP Address:      192.168.1.245  [44-47]
  Dest. IP Address:       192.168.1.2  [48-51]
  No IP Options

ICMP - Internet Control Messages Protocol
  ICMP Type:              0  Echo Reply  [52]
  Code:                   0  [53]
  Checksum:               0x9C50  [54-55]
  Identifier:             0x0300  [56-57]
  Sequence Number:        0x0BB6  [58-59]
  ICMP Data Area:         32 bytes
  abcdefghijklmnop  61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  [60-75]
  qrstuvwabcdefghi  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  [76-91]
FCS - Frame Check Sequence
  FCS:                    0xDFFB7603  [92-95]
```

Figure 51. Decoded Data Packet

As we see, the transmission rate of this packet was 24 Mbps and its total length was 96 bytes or else it was $96 \times 8 = 768$ bits, which are shown in the red numbers. As we have already mentioned, the pure data of the ping packet consisted only of 32 bytes or $32 \times 8 = 256$ bits, printed in green. Thus, the rest $(768 - 256) = 512$ bits were indispensable overhead bits. By computing the total time t_{total} that the packet needed to be transmitted, we found that $t_{total} = (96 \times 8)/(24 \times 10^6)$ s $= 32$ μs. This period of time was also the time for the pure data bits to be transmitted. That is, the ping data bits were transmitted with an actual throughput rate $R_{throughput} = (32 \times 8)/(32 \times 10^{-6})$ Bps $= 8$ Mbps. Thus, the computed actual outdoor throughput of the 802.11g suffered a reduction of 65% of the measured Average Data Rate presented in Table 25 above. This means that the maximum pure data rate achieved in the 802.11g outdoor WLAN is about 15 Mbps (approximately

28.6 % of the maximum advertised value) at close distances from the AP, and it decreases up to under 0.5 Mbps at great distances. We should note that this experimental calculation was based on the transmission of small data packets (32 bytes).

According to [20] and [21] the maximum data throughput rate of 802.11g is between 24 and 27 Mbps. These results were based on the 54-Mbps maximum theoretical transmission rate. Thus, the 802.11g actual transmission rate will suffer a reduction of 60%. Since the results we extracted consider both the data packet rate and the ACK packet rate and since we used as maximum rate the 40 Mbps, we realize that our results are very similar to those referred to in [20] and in [21].

Next, the advertised 802.11g data link performance from Cisco [19] was compared with the measured results. Table 26 below shows the outdoor range for the AP 1200 using an omni-directional antenna with +5 dBi gain that Cisco advertises.

Data Link Rate	Outdoor Range
54 Mbps	76 m
18 Mbps	183 m
6 Mbps	396 m

Table 26. Cisco Aironet AIR-CB20A Outdoor Range (After Ref. 19.)

Comparing the data measured from D-Link system, we noticed that the advertised transmission rates were greater, probably because they did not consider the ACK packet rate. It is interesting to note that at the 183-meter point, the theoretical rate (18 Mbps) was much less than the measured one (about 25 Mbps). This might have happened due to the multipath effect, which in this case acted positively and not negatively, as we should expect.

E. SUMMARY

Summarizing all the above results, by using an 802.11g WLAN, we achieved a maximum transmission rate of pure data up to 15 Mbps. This rate is, of course, much less than the advertised rate of 54 Mbps. But the 15 Mbps rate referred to the clear data transmission rate, and it included the ACK for a data packet. Thus we have obtained a really high-rate network which, of course, could be very helpful during military operations.

Another important result was that, for a very optimistic situation, we were capable of establishing and maintaining an 802.11g WLAN up to 400 m. Naturally, the battlefield of a military operation would probably not be similar to Figure 19. The multipath effect would be more severe, and generally the transmission distances would be reduced. As a result, we should maintain close proximity of the "wireless clients" and the transmitting AP in order to maintain our high-speed wireless network.

In addition, by using the new state-of-the art Wi-Fi security mechanism, namely WPA, we can make sure that our network will be as secure as possible.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND FUTURE WORK

The basic purpose of this research was to develop a prototype system able to detect and to process 802.11g-compliant WLAN signals. We accomplished this by using commercially available low-cost hardware and software solutions.

This experimental evaluation could be a useful guideline for implementing 802.11g in military operations for which the need for a high-speed network is immediate.

Initially we posed the following three main questions and developed our research by seeking answers to them:

- What are the most appropriate commercially available low-cost hardware and software solutions that can be used to process wireless IEEE 802.11g signals?
- If we built the prototype system using the selected hardware and software solutions, what is the effective detection range of that system?
- Having created a "virtual 802.11g WLAN" what is the measured operating range of 802.11g networks, compared to the actual throughput rate and to the advertised operating range?

A. CONCLUSIONS

Chapter II initially presented a general description of some important features of the IEEE 802.11 standard. The old and newer security implementations (WEP and WPA) were the most important of them. After that, we briefly analyzed the latest IEEE standard 802.11g noting the differences and the compatibilities with the former IEEE standards, 802.11a and 802.11b. Finally the two path-loss models, which were most suitable for our case, were considered. They were used as a guideline for the rest of the chapters.

Chapter III set the important requirements for the prototype system. Then according to these requirements, we selected both the software and hardware solutions that we needed. Several measurements were performed on available hardware to choose the best 802.11g wireless card for the prototype system. The resulting prototype system, with a total cost of $5,650, was described at the end of Chapter III.

In Chapter IV, the newly designed prototype system was tested so that we could make sure it performed well. For that reason, we implemented three available systems:

the Linksys, the Orinoco and the D-Link systems. The evaluation of the prototype system was based on the captured data that these systems transmitted. Thus, according to the performance results, the prototype system was very reliable with a maximum PER of about 13% at the maximum range of 395 m. So, the prototype system proved useful for implementation in a military WLAN network. However, the system might be of limited use to detect and to process other 802.11g WLAN beyond 400 m. Unfortunately 400 m is not a great distance on a modern battlefield. The operable range will be even shorter if the system is used in any area of intense multi-path environment.

In Chapter V, we developed the final point of the thesis and we computed the effective range of the 802.11g network and the actual data throughput in order to decide whether an 802.11g network could be used for military operations. The prototype system was used as an independent detection tool at several positions to capture the data link rate achieved by three different 802.11g systems. The measurement results concluded that the 802.11g network could provide up to 20 Mbps of data link rate for distances up to 200 m while the data link rate degraded (1 Mbps or lower) at the range of 400 m. The most interesting result was that the maximum pure data throughput was 15 Mbps at the range of 70 m from the wireless source. Even though it was much lower that the advertised 54 Mbps, this rate was still very high.

This high data rate of the 802.11g network would therefore be very useful in operations in which a high-speed wireless data exchange is required within a small operational radius of up to 200 m, without security being an important issue.

B. FUTURE WORK

1. Effect of WPA Encryption Mechanism on 802.11g Performance

All tests were performed under the infrastructure mode with or without WEP encryption. The experimental measurements showed that while the use of 64-bit WEP has almost no effect on the transmission rate, the use of 128-bit WEP decreases the transmission rate about 10% to 15% and with a maximum value of 5 Mbps at the maximum effective range of 400 m. Also, the PER increased as we increased the security feature to 128-bit WEP.

It would be interesting to investigate the effect of the WPA encryption mechanism on the performance of the 802.11g. More specifically, we should determine if the use of the WPA has a significant or insignificant effect on the transmission rate, on the PER of the 802.11g and on the performance of the prototype system we built.

2. Extending the Range Performance of the Prototype System Using External Antennas

As concluded earlier, the detection range of the prototype system was absolutely limited by the sensitivity of the commercial 802.11g receiver cards that were used. We might significantly extend the detection range of the prototype system if we implemented an external antenna with a high gain combined with an appropriate amplifier. With this improvement the prototype system could be even more efficient in military operations.

3. Ability of the System in a Multi-Path Environment

During our experimental study, we evaluated the performance of the newly developed prototype system only on a flat environment. Such an environment has no significant multipath effect on the signal path loss. Since the modern battlefield would most probably be a multipath environment, it would be an interesting extension to this research to determine whether the prototype system is efficient enough, even when it operates in a "severe multipath environment."

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. LAN MAN Standards Committee of the IEEE Computer Society, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* ANSI/IEEE Std 802.11, [http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=14251], last accessed July 2004.

2. LAN MAN Standards Committee of the IEEE Computer Society, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHZ Band,* ANSI/IEEE Std 802.11a [http://ieeexplore.ieee.org/iel5/6606/17645/00815305.pdf?isNumber=17645&prod=STD&arnumber=815305&arSt=&ared=&arAuthor=], last accessed July 2004.

3. IEEE Standard for Information Technology, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band,* ANSI/IEEE Std 802.11g, [http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=27242], last accessed July 2004.

4. Jesse R. Walker, "Unsafe at Any Key Size: An Analysis of WEP Encapsulation," IEEE 802.11 Wireless LANs, [http://www.dis.org/wl/pdf/unsafe.pdf], last accessed July 2004.

5. Sangram Gayal and Dr.S.A.Manickam, "Wireless LAN Security," [http://hyatus.dune2.info/Wireless_802.11/wireless-lan-security.pdf], last accessed July 2004.

6. Stanley Wong, *"*The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards," [http://www.sans.org/rr/papers/68/1109.pdf], last accessed July 2004.

7. IEEE Standard for Information Technology, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band,* ANSI/IEEE Std 802.11b, [http://ieeexplore.ieee.org/iel5/6642/17714/00817038.pdf?isNumber=17714&prod=STD&arnumber=817038&arSt=i&ared=90&arAuthor=], last accessed July 2004

8. Theodore S. Rappaport, *Wireless Communications – Principles and Practice (Second Edition)*, Prentice Hall, New Jersey, 2002.

9. Che Seng Goh, "Prototype System for Detecting and Processing IEEE 80211a Signals," Master's Thesis, Naval Postgraduate School, Monterey, California, March 2004.

10. Walter N. Currier Jr., "Prototype System for Detecting and Processing IEEE 80211b Signals," Master's Thesis, Naval Postgraduate School, Monterey, California, March 2002.

11. NetWork Instruments Inc., "Expert Observer Pricing," [http://www.networkinstruments.com/purchasing/us_obs_pricing.html], last accessed June 2004.

12. Wildpackets Inc., "AiroPeek NX Special Maintenance Owner Pricing," [http://www.wildpackets.com/purchase/products/apnx], last accessed June 2004.

13. Linksys, "WPC-54G - Instant Wireless™ PC Card," [http://www.linksys.com/products/product.asp?grid=33&scid=36&prid=642], last accessed June 2004.

14. Proxim, "ORiNOCO 11a/b/g ComboCard," [http://www.proxim.com/products/wifi/client/abgcard], last accessed June 2004.

15. D-Link Inc., "D-Link AirPlus XtremeG DWL-650 Wireless Adapter," [http://www.dlink.com/products/resource.asp?pid=15&rid=58], last accessed June 2004.

16. Linksys, "Linksys WAP54G Access Point," [http://www.linksys.com/products/product.asp?action=zoom&prid=505&scid=35], last accessed June 2004.

17. Garmin, "*e*trex GPS," [http://www.garmin.com/manuals/42_OwnersManual.pdf], last accessed July 2004.

18. Proxim, "ORiNOCO AP-2000 11g Kit," [http://www.proxim.com/learn/library/datasheets/AP2000_11g_kit.pdf], last accessed July 2004.

19. Cisco Inc., "Cisco Aironet 1200 Series Access Point," [http://www.cisco.com/en/US/products/hw/wireless/ps430/products_data_sheet09186a00800937a6.html], last accessed July 2004.

20. Broadcom White papers, "IEEE 802.11g, The New Mainstream Wireless LAN Standard," [http://www.broadcom.com/collateral/wp/802.11g-WP104-R.pdf], last accessed July 2004.

21. Proxim White Pares, "Maximizing Your 802.11g Investment," [http://www.proxim.com/learn/library/whitepapers/maximizing_80211g_investment.pdf], last accessed July 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chairman, Code EC/Po
   Department of Electrical and Computing Engineering
   Naval Postgraduate School
   Monterey, California

4. Chairman, Code IS/Bo
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Professor Tri T. Ha, Code EC/Ha
   Department of Electrical and Computing Engineering
   Naval Postgraduate School
   Monterey, California

6. Professor David C. Jenn, Code EC/Jn
   Department of Electrical and Computing Engineering
   Naval Postgraduate School
   Monterey, California

7. Embassy of Greece, Naval Attaché
   Washington, DC

8. Cryptologic Research Laboratory
   ATTN: Nathan Beltz
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

9. Georgios Kypriotis
   Grigoriou Lampraki 144
   Pireas, GREECE
   TK: 185-35